

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 8 月 25 日 (25.08.2005)

PCT

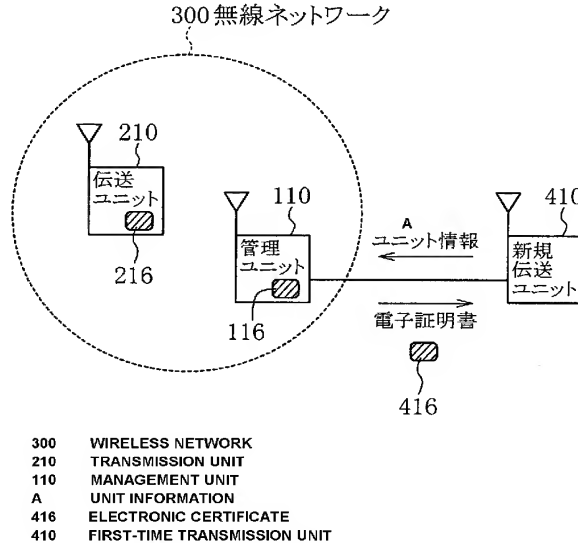
(10) 国際公開番号
WO 2005/078990 A1

- (51) 国際特許分類⁷: H04L 9/08, 12/28 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/016388 (75) 発明者/出願人 (米国についてのみ): 笠浦 毅
(22) 国際出願日: 2004 年 11 月 5 日 (05.11.2004) (KASURA, Tsuyoshi) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 井上 禎之 (INOUE, Sadayuki) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 松本 壮一郎 (MATSUMOTO, Soichiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 志田 哲郎 (SHIDA, Tetsuro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 佐藤 利光 (SATO, Toshimitsu) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 辻下 雅啓 (TSUJISHITA, Masahiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 Tokyo (JP).
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ:
特願2004-038000 2004 年 2 月 16 日 (16.02.2004) JP
(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 Tokyo (JP).

[続葉有]

(54) Title: DATA TRANSMITTING/RECEIVING APPARATUS AND ELECTRONIC CERTIFICATE ISSUING METHOD

(54) 発明の名称: データ送受信装置及び電子証明書発行方法



(57) Abstract: A management unit (110), which issues an electronic certificate to a first-time transmission unit (410), has a wireless communication part that communicates in a network (300) and also has a wire communication part to which the first-time transmission unit (410) can be connected. When the first-time transmission unit (410) is wire-connected to the management unit (110), the management unit (110) determines, based on received device type information of the first-time transmission unit (410), whether the first-time transmission unit (410) has any communication means capable of communicating in the network (300). If so determining, the management unit (110) uses a device identifier specific to the first-time transmission unit (410) to make an electronic certificate, and then transmits it to the first-time transmission unit (410).

(57) 要約: 新規伝送ユニット (410) に対して電子証明書を発行する管理ユニット (110) は、ネットワーク (300) における通信を行う無線通信部と新規伝送ユニット (410) を接続することができる有線通信部を有し、新規伝送ユニット (410) が管理ユニット (110)

[続葉有]

WO 2005/078990 A1



千代田区丸の内二丁目2番3号 三菱電機株式会社
内 Tokyo (JP).

(74) 代理人: 前田実, 外(MAEDA, Minoru et al.); 〒
1510053 東京都渋谷区代々木2丁目16番2号 甲
田ビル4階 前田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が
可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,
LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA,
NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,
SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可
能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,
SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,
KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,
IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE,
SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

に有線接続されたときに、受信した新規伝送ユニット(410)の機器種別情報に基づいて新規伝送ユニット
(410)がネットワーク(300)において通信可能な通信手段を備えた機器であるか否かを識別し、そのよう
な手段を備えた機器であると識別した場合に、新規伝送ユニット(410)に固有の機器識別子を用いて電子証明
書を作成し、電子証明書を新規伝送ユニット(410)に送信する。

明 細 書

データ送受信装置及び電子証明書発行方法

技術分野

- [0001] 本発明は、電子証明書を所有するデータ送受信装置から構成されるネットワークに新規データ送受信装置を参加させる際に、新規データ送受信装置に対して電子証明書を発行する方法、及び、この方法を実施するデータ送受信装置に関するものである。

背景技術

- [0002] IEEE802. 11規格は、無線LAN(Local Area Network)の機器認証方法として、オープンシステム(Open System)認証とシェアードキー(Shared Key)認証を規定している。オープンシステム認証は、無線端末間における認証フレームの交換を規定するが、認証を要求するすべての端末を許可するので、悪意ある第三者からの不正アクセスを防止できない。シェアードキー認証は、無線端末間においてシェアードキー(Shared Key:共有鍵)となるパスフレーズを予め共有しておくことを規定するが、共有方法については規定していない。一般的には、利用者が、口頭による通知や電子メールによる配布によってシェアードキーを入手し、無線端末にシェアードキーとなるパスフレーズを設定する。
- [0003] また、無線LANのセキュリティ強化を目的としたIEEE802. 11i規格やWPA(Wi-Fi Protect Access)規格は、RADIUS(Remote Authentication Dial In User Service:ラディウス)等の認証サーバを利用した機器認証を規定している。認証を要求する無線端末は、有線ネットワークに接続された基地局に対して無線で認証要求を送信し、基地局は、有線ネットワーク内に存在する認証サーバに対して有線で認証の可否を問い合わせる。無線端末が認証されるためには、この認証サーバに対して、予めMAC(Media Control Access)アドレス等の端末情報を登録しておく必要がある。
- [0004] さらにまた、下記の特許文献1には、無線通信による公開鍵暗号方式を利用した無線端末情報の登録についての開示がある。

[0005] また、下記の特許文献2には、共通情報を共有することによって、同一の共通情報を所有する端末同士をグループ化し、グループリストを参照することで、端末間の認証を行う技術についての開示がある。

[0006] また、下記の特許文献3には、予め各端末に設定された公開鍵証明書を用いて、基地局(AP)が所有するMACアドレスリストに基づいた公開鍵認証を行う技術についての開示がある。

[0007] 特許文献1:特開2002-159053号公報

特許文献2:特開2003-198544号公報

特許文献3:特開2003-005641号公報

発明の開示

発明が解決しようとする課題

[0008] しかしながら、上記したいずれの方法においても、登録情報の授受が、第三者からの不正アクセスに対して確実に安全であると認識できるような通信手段で行われておらず、盗聴や改ざんによる‘なりすまし’がなされるおそれがあるという問題があった。

[0009] また、無線端末に対するパスフレーズの設定や、認証サーバへの端末情報の設定を行うのは端末の利用者であるが、一般家庭の利用者がこのような操作を行うことは困難であるという問題があった。

[0010] そこで、本発明は、上記したような従来技術の課題を解決するためになされたものであり、その目的は、電子証明書を所有するデータ送受信装置から構成されるネットワークに新規データ送受信装置を参加させる際に、外部からの不正アクセスに対するセキュリティを確保しつつ、容易な操作によって新規データ送受信装置に対して電子証明書を発行する方法及びこの方法を実施するデータ送受信装置を提供することにある。

課題を解決するための手段

[0011] 本発明のデータ送受信装置は、ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行するデータ送受信装置であって、前記ネットワークにおける通信を行う第1の通信部と、前記新

規データ送受信装置を接続することができる第2の通信部と、前記電子証明書の発行処理を行う制御部とを有し、前記制御部は、前記新規データ送受信装置が前記第2の通信部に接続されたときに、前記新規データ送受信装置から前記第2の通信部を経由して受信した前記新規データ送受信装置の機器種別情報に基づいて、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であるか否かを識別し、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であると識別した場合に、前記新規データ送受信装置から前記第2の通信部を経由して受信した前記新規データ送受信装置に固有の機器識別子を用いて電子証明書を作成し、前記作成された電子証明書を前記第2の通信部を経由して前記新規データ送受信装置に送信するように制御するものである。

- [0012] 他の発明のデータ送受信装置は、ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行するデータ送受信装置であって、前記ネットワークにおける通信を行う通信部と、前記電子証明書の発行処理を行う制御部とを有し、前記制御部は、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器である場合には、前記新規データ送受信装置から、前記新規データ送受信装置が接続されたデータ送受信装置及び前記通信部を経由して前記電子証明書に記載するための機器識別子を受信し、前記機器識別子を用いて前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記通信部及び前記新規データ送受信装置が接続されたデータ送受信装置を経由して前記新規データ送受信装置に送信するように制御するものである。

発明の効果

- [0013] 本発明によれば、電子証明書を所有するデータ送受信装置から構成されるネットワークに新規データ送受信装置を参加させる際に、外部からの不正アクセスに対するセキュリティを確保しつつ新規データ送受信装置に対して電子証明書を発行することができるという効果が得られる。

[0014] また、本発明によれば、電子証明書を所有するデータ送受信装置に新規データ送受信装置を接続するという容易な操作により電子証明書を取得することができるという効果が得られる。

図面の簡単な説明

[0015] [図1]本発明の実施の形態1及び2に係る電子証明書発行方法を実施する構成を示す図である。

[図2]図1の管理ユニットの構成を概略的に示すブロック図である。

[図3]図1の電子証明書発行を要求する新規伝送ユニットの構成を概略的に示すブロック図である。

[図4]図1の伝送ユニットの構成を概略的に示すブロック図である。

[図5]実施の形態1に係る電子証明書発行方法を説明するための構成図である。

[図6]実施の形態1に係る電子証明書発行方法の手順を示す図である。

[図7]実施の形態1に係る電子証明書発行方法における管理ユニットの動作を示すフローチャートである。

[図8]図7の機器識別処理を示すフローチャートである。

[図9]図7の電子証明書所有確認処理を示すフローチャートである。

[図10]実施の形態1に係る電子証明書発行方法における新規伝送ユニットの動作を示すフローチャートである。

[図11]実施の形態2に係る電子証明書発行方法を説明するための構成図である。

[図12]実施の形態2に係る電子証明書発行方法の手順を示す図である。

[図13]実施の形態2に係る電子証明書発行方法における管理ユニットの動作を示すフローチャートである。

[図14]実施の形態2に係る電子証明書発行方法における中継用の伝送ユニットの動作を示すフローチャート(その1)である。

[図15]実施の形態2に係る電子証明書発行方法における中継用の伝送ユニットの動作を示すフローチャート(その2)である。

符号の説明

[0016] 100, 200 有線ネットワーク、 110 管理ユニット、 116 電子証明書、 120, 2

20, 230 接続機器、210 伝送ユニット、216 電子証明書、300 無線ネットワーク、410 新規伝送ユニット、416 電子証明書。

発明を実施するための最良の形態

[0017] 実施の形態1.

図1は、本発明の実施の形態1に係る電子証明書発行方法を実施する構成を示す図である。図1に示されるネットワーク300は、ネットワーク参加権限を証明するデータである電子証明書116, 216を用いることにより悪意ある第三者からの不正アクセスに対するセキュリティが確保されたネットワークであり、例えば、IEEE802. 11ネットワークである。実施の形態1において、ネットワーク300は、電波又は赤外線等により通信をする無線ネットワークである。無線ネットワーク300は、ネットワーク参加権限を証明する電子証明書を発行するデータ送受信装置である管理ユニット(ネットワーク管理機能を持つ伝送ユニット)110と、他のデータ送受信装置である伝送ユニット210とから構成されている。ただし、無線ネットワークを構成する伝送ユニットの数は2台に限定されず、何台であってもよい。管理ユニット110は、無線ネットワーク300への参加権限を証明する電子証明書116を所有し、伝送ユニット210は、無線ネットワーク300への参加権限を証明する電子証明書216を所有している。

[0018] また、図1において、ネットワーク100及び200はそれぞれ、悪意ある第三者からの不正アクセスに対して、利用者が明らかに安全であると認識できる通信手段によって構成されたネットワークであり、例えば、IEEE1394ネットワークである。実施の形態1において、ネットワーク100及び200は、有線ネットワークである。有線ネットワーク100は、管理ユニット110と、管理ユニット110に通信ケーブル等を用いて有線接続された機器120から構成されている。また、有線ネットワーク200は、伝送ユニット210と、伝送ユニット210に通信ケーブル等を用いて有線接続された機器220及び230から構成されている。なお、図1においては、機器220, 230が伝送ユニット210に直接接続されている場合が示されているが、伝送ユニット210、機器220、及び機器230をシリーズに接続してもよい。なお、各伝送ユニット110, 210, 410は、例えば、携帯電話装置、パーソナルコンピュータ(PC)、PC周辺機器、映像機器(放送受信機、映像記録再生装置、映像表示装置等)のような、無線通信機能を備えた通信機器であ

る。また、有線ネットワーク100及び200の構成は、図1に示された構成に限定されない。

[0019] 有線ネットワーク100内の機器120が、無線ネットワーク300を経由して、有線ネットワーク200内の機器220及び230とデータ通信を行う場合の動作を説明する。機器120から送信されたデータは、通信ケーブルを経由して管理ユニット110によって受信される。データを受信した管理ユニット110は、伝送ユニット210に対して電子証明書の提示を要求し、伝送ユニット210により提示された電子証明書216を受信することによって、伝送ユニット210が無線ネットワーク300に参加する権限を有する機器であることを認証する。また、伝送ユニット210は、管理ユニット110に対して電子証明書の提示を要求し、管理ユニット110により提示された電子証明書116を受信することによって、管理ユニット110が無線ネットワーク300に参加する権限を有する機器であることを認証する。管理ユニット110と伝送ユニット210の相互認証が完了した後、管理ユニット110は、機器120から受信したデータを無線ネットワーク300による無線通信により伝送ユニット210へ送信する。データを受信した伝送ユニット210は、通信ケーブルを経由して機器220及び230にデータを送信する。また、機器220又は230から機器120にデータを送信する場合にも、同様の手順によりデータを送信することができる。以上の手順により、有線ネットワーク100内の機器120と、有線ネットワーク200内の機器220及び230とは、無線ネットワーク300を経由して、データ通信を行うことができる。なお、図1において、新規伝送ユニット410は、無線ネットワーク300への参加権限を証明する電子証明書を所有していないので、管理ユニット110又は伝送ユニット210との間で無線によるデータ通信を行うことはできない。

[0020] 図2は、管理ユニット110の構成を概略的に示すブロック図である。図2に示されるように、管理ユニット110は、無線ネットワーク300への参加権限を証明する電子証明書116を所有する。図2に示されるように、管理ユニット110は、無線ネットワーク300における通信を行う無線通信部111（例えば、IEEE802.11規格に準拠する無線LAN回路）と、機器120及び新規伝送ユニット410のいずれか一方又は両方を有線接続することができる有線通信部112（例えば、IEEE1394規格に準拠するインタフェース回路）と、液晶画面や表示ランプ等の表示部113と、半導体メモリ等の記憶部

114と、装置全体の動作を制御する制御部115とを有する。管理ユニット110は、無線ネットワーク300に新規伝送ユニット410を参加させる際に、新規伝送ユニット410に対して電子証明書を発行する。管理ユニット110は、電子証明書発行時に、例えば、電子証明書発行用ソフトウェアに基づいて動作する。

[0021] 図3は、伝送ユニット210の構成を概略的に示すブロック図である。図3に示されるように、伝送ユニット210は、無線ネットワーク300への参加権限を証明する電子証明書216を所有する。図3に示されるように、伝送ユニット210は、無線ネットワーク300における通信を行う無線通信部211(例えば、IEEE802.11規格に準拠する無線LAN回路)と、機器220、230及び新規伝送ユニット410の一つ以上を有線接続することができる有線通信部212(例えば、IEEE1394規格に準拠するインタフェース回路)と、液晶画面や表示ランプ等の表示部213と、半導体メモリ等の記憶部214と、装置全体の動作を制御する制御部215とを有する。

[0022] 図4は、新規伝送ユニット410の構成を概略的に示すブロック図である。図4に示されるように、新規伝送ユニット410は、当初は、無線ネットワーク300への参加権限を証明する電子証明書を所有していない。図4に示されるように、新規伝送ユニット410は、無線ネットワークにおける通信を行う無線通信部411(例えば、IEEE802.11規格に準拠する無線LAN回路)と、管理ユニット110等と有線接続することができる有線通信部412(例えば、IEEE1394規格に準拠するインタフェース回路)と、液晶画面や表示ランプ等の表示部413と、半導体メモリ等の記憶部414と、装置全体の動作を制御する制御部415とを有する。新規伝送ユニット410は、電子証明書発行を受けるときに、例えば、電子証明書発行要求用ソフトウェアに基づいて動作する。

[0023] 図5は、実施の形態1に係る電子証明書発行方法を説明するための構成図である。図5を用いて、無線ネットワーク300への参加権限を証明する電子証明書を所有していない新規伝送ユニット410が、管理ユニット110から無線ネットワーク300への参加権限を証明する電子証明書416の発行を受けるための動作の概略を説明する。

[0024] 先ず、利用者は、新規伝送ユニット410の有線通信部412と、管理ユニット110の有線通信部112とを、例えば、IEEE1394規格に準拠した通信ケーブルによって接続する。利用者は、新規伝送ユニット410の有線通信部412と、管理ユニット110の

有線通信部112とを、通信ケーブルによって接続することによって、新規伝送ユニット410と管理ユニット110とを、悪意ある第三者からの不正アクセスに対して、利用者が明らかに安全であると認識することができる。

[0025] 新規伝送ユニット410が接続された後、管理ユニット110は、新規伝送ユニット410の機器種別情報を受信する。管理ユニット110は、新規伝送ユニット410の機器種別情報に基づいて、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた機器であるか否かを識別する。また、管理ユニット110は、新規伝送ユニット410に固有の機器情報である機器識別子(ユニット情報)を受信する。

[0026] 管理ユニット110は、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた機器であると識別した場合に、新規伝送ユニット410の機器識別子を用いて電子証明書416を作成し、作成された電子証明書416を新規伝送ユニット410に送信する。以上により、管理ユニット110による、新規伝送ユニット410に対する電子証明書416の発行処理が終了する。

[0027] 図6は、実施の形態1に係る電子証明書発行方法の手順を示す図である。以下に、図6に基づいて、新規伝送ユニット410を、電子証明書を発行する管理ユニット110に接続したときの電子証明書授受動作について説明する。

[0028] 実施の形態1においては、管理ユニット110及び新規伝送ユニット410は、各々現在の状況を利用者へ通知するための表示部として、緑(G)ランプ及び赤(R)ランプを備えている。図におけるランプ状態の記載方法を、以下の項目(1)〜(5)に解説する。

(1)「破線丸印のみの記号」は、ランプ無灯状態を示し、伝送ユニットが電子証明書を所有していない場合を示す。

(2)「Gを破線丸印で囲う記号」は、Gランプ点滅状態を示し、伝送ユニットが電子証明書を所有しているが、無線ネットワーク300に参加していない場合を示す。

(3)「Gを実線丸印で囲う記号」は、Gランプ点灯状態を示し、伝送ユニットが電子証明書を所有しており、かつ、無線ネットワーク300に参加している場合を示す。

(4)「Rを破線丸印で囲う記号」は、Rランプ点滅状態を示し、電子証明書発行処理の途中であることを示す。

(5)「Rを実線丸印で囲う記号」は、Rランプ点灯状態を示し、電子証明書発行処理が異常終了して電子証明書が発行されなかったことを示す。

なお、図6において、管理ユニット110と新規伝送ユニット410とを繋ぐ横方向の実線矢印は、有線通信であることを示している。

[0029] 図6に示されるように、電子証明書の発行に際しては、先ず、管理ユニット110と新規伝送ユニット410を通信ケーブルで有線接続する(ステップS1000)。このとき、管理ユニット110は電子証明書116を所有しており、かつ、無線ネットワーク300に参加しているので、管理ユニット110の表示部はGランプ点灯状態である。一方、新規伝送ユニット410は電子証明書を所有しておらず、無線ネットワーク300へ参加していないので、新規伝送ユニット410の表示部はランプ無灯状態である。

[0030] 次に、管理ユニット110は、有線接続された機器(新規伝送ユニット410)が無線ネットワーク300において通信可能な通信手段を備えた伝送ユニットであるかどうかを識別する(ステップS1001)。この機器識別ステップの詳細は後述する(図7のステップS1103及び図8)。

[0031] 次に、管理ユニット110は、有線接続された新規伝送ユニット410が既に電子証明書を所有しているかどうかを確認する(ステップS1002)。この電子証明書所有確認ステップの詳細は後述する(図7のステップS1104及び図9)。

[0032] 次に、管理ユニット110は、新規伝送ユニット410に対して、電子証明書発行フローの開始を通知する開始通知を送信し、タイマ1を起動する(ステップS1003)。開始通知を受信した新規伝送ユニット410は、新規伝送ユニット410の表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知する。

[0033] 次に、新規伝送ユニット410は、管理ユニット110に対して電子証明書発行要求を送信し、タイマ2を起動する(ステップS1004)。電子証明書発行要求を受信した管理ユニット110は、管理ユニット110の表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知し、タイマ1を終了する。管理ユニット110は、タイマ1がタイムアウトする前に電子証明書発行要求を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図7のステップS1117〜S1121)。

- [0034] タイマ1がタイムアウトする前に電子証明書発行要求を受信した管理ユニット110は、新規伝送ユニット410に対して、電子証明書に記載するための新規伝送ユニット410に固有のユニット情報を得るために、ユニット情報要求を送信し、タイマ3を起動する(ステップS1005)。ユニット情報要求を受信した新規伝送ユニット410は、タイマ2を終了する。新規伝送ユニット410は、タイマ2がタイムアウトする前に、ユニット情報要求を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図10のステップS1419〜S1423)。
- [0035] タイマ2がタイムアウトする前にユニット情報要求を受信した新規伝送ユニット410は、管理ユニット110に対してユニット情報を送信し、タイマ4を起動する(ステップS1006)。ユニット情報としては、MAC(Media Control Access)アドレス等の伝送ユニットに固有の機器識別子が挙げられる。ユニット情報を受信した管理ユニット110は、タイマ3を終了する。管理ユニット110は、タイマ3がタイムアウトする前にユニット情報を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図7のステップS1117〜S1121)。
- [0036] タイマ3がタイムアウトする前にユニット情報を受信した管理ユニット110は、受信したユニット情報を基に電子証明書を作成し、新規伝送ユニット410に対して電子証明書を発行し、タイマ5を起動する(ステップS1007)。電子証明書を受信した新規伝送ユニット410は、タイマ4を終了する。新規伝送ユニット410は、タイマ4がタイムアウトする前に電子証明書を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図10のステップS1419〜S1423)。
- [0037] タイマ4がタイムアウトする前に電子証明書を受信した新規伝送ユニット410は、受信した電子証明書の内容を検証し、電子証明書の正当性を確認(例えば、第三者機関である電子証明書認証局による正当性の検証を受ける等)した場合には、管理ユニット110に対して、電子証明書を正常に受領したことを通知する電子証明書発行応答を送信し、タイマ6を起動する(ステップS1008)。新規伝送ユニット410は、電子証明書の内容が不当である場合には、電子証明書発行応答に再度ユニット情報を含めて送信する。電子証明書発行応答を受信した管理ユニット110は、タイマ5を終了し、管理ユニット110の表示部を元のGランプ点灯状態へ戻す。新規伝送ユニット

410は、タイマ5がタイムアウトする前に電子証明書発行応答を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図10のステップS1419〜S1423)。

[0038] タイマ5がタイムアウトする前に電子証明書発行応答を受信した管理ユニット110は、発行した電子証明書の正当性が確認された場合には、新規伝送ユニット410に対して電子証明書発行フローを終了させる終了通知を送信する(ステップS1008)。終了通知を受信した新規伝送ユニット410は、タイマ6を終了する。新規伝送ユニット410は、タイマ6がタイムアウトする前に終了通知を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図10のステップS1419〜S1423)。図6のステップS1008において、電子証明書発行応答を受信した管理ユニット110は、発行した電子証明書が不当である場合には、受信した電子証明書発行応答に含まれるユニット情報を基に再度電子証明書を作成し、処理をステップS1006へ戻し、新規伝送ユニット410に対して再度電子証明書を発行する。

[0039] タイマ6がタイムアウトする前に終了通知を受信した新規伝送ユニット410は、新規伝送ユニット410の表示部をGランプ点滅状態に切替えて、電子証明書発行フローが正常に終了して、電子証明書が取得できたことを利用者へ通知する。利用者はGランプ点滅状態を確認して、管理ユニット110と新規伝送ユニット410との有線接続を切断することができる(ステップS1010)。新規伝送ユニット410は、タイマ6がタイムアウトする前に終了通知を受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図10のステップS1419〜S1423)。

[0040] 以上の処理フローにより、新規伝送ユニット410は、管理ユニット110から図5で示す無線ネットワーク300へ参加するための電子証明書416を取得することができる。

[0041] 図7は、管理ユニット110へ有線接続された新規伝送ユニット410に対して、管理ユニット110が電子証明書を発行する手順を示すフローチャートである。また、図8は、図7のステップS1103の機器識別処理を示すフローチャートであり、図9は、図7のステップS1104の電子証明書所有確認処理を示すフローチャートである。図7から図9までを用いて、実施の形態1における管理ユニット110の動作を詳細に説明する。

[0042] 図7に示されるように、電子証明書発行処理の開始時(ステップS1100)には、管理

ユニット110は、電子証明書を所有しており、かつ、無線ネットワーク300へ参加しているので、管理ユニット110の表示部はGランプ点灯状態である(ステップS1101)。次に、利用者は、管理ユニット110と新規伝送ユニット410を、利用者が確実にネットワークセキュリティ上安全であると認識できる有線により接続する(ステップS1102)。

[0043] 次に、管理ユニット110は、有線接続された新規伝送ユニット410が無線ネットワーク300と通信可能な通信手段を備えた伝送ユニットであるか否かを識別するための処理を実行する(図7のステップS1103、及び、図8のステップS1200〜S1208)。

[0044] 図8のステップS1201において、管理ユニット110が、接続された新規伝送ユニット410から、所定時間内に機器識別要求を受信した場合は、接続された新規伝送ユニット410に対して、新規伝送ユニット410が無線ネットワーク300に参加可能な(すなわち、無線ネットワーク300において通信可能な通信手段を備えた)伝送ユニットであることを示す機器識別応答を送信して(ステップS1202)、機器識別フローを終了する(ステップS1206)。ステップS1206における機器識別フローの終了は、新規伝送ユニット410が無線ネットワーク300において通信可能な伝送ユニットであることを示すものであり、ネットワーク参加可能終了(図では「OK終了」と言う)。

[0045] 図8のステップS1201において、管理ユニット110は、接続された新規伝送ユニット410から、所定時間内に機器識別要求を受信しなかった場合は、新規伝送ユニット410に対して機器識別要求を送信する(ステップS1203)。図8のステップS1204において、管理ユニット110は、接続された新規伝送ユニット410から、所定時間内に機器識別応答を受信した場合は、機器識別応答を検証し(ステップS1205)、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた伝送ユニットである場合には、機器識別フローをネットワーク参加可能終了(OK終了)する(ステップS1206)。図8のステップS1205において、管理ユニット110は、機器識別応答を検証して(ステップS1205)、新規伝送ユニット410が無線ネットワーク300において通信可能な伝送ユニットでない場合には、機器識別フローを終了する(ステップS1207)。ステップS1207における機器識別フローの終了は、新規伝送ユニット410が無線ネットワーク300において通信可能な伝送ユニットではないことを示すものであり、ネットワーク参加不可終了(図では「NG終了」と言う)。

- [0046] 図8のステップS1204において、管理ユニット110は、送信した機器識別要求に対する機器識別応答を、接続された機器から所定時間内に機器識別応答を受信しない場合は、タイムアウトと判定し、機器識別フローを終了とする(ステップS1208)。ステップS1208における機器識別フローの終了は、新規伝送ユニット41が無線ネットワーク300において通信可能な伝送ユニットであるかどうかの識別結果を管理ユニット110が受け取ることができなかったことを示すものであり、「エラー終了」と言う。
- [0047] 図7のステップS1103において、機器識別フローがネットワーク参加不可終了(NG終了)の場合は、接続された機器は無線ネットワーク300における通信が可能な伝送ユニットではなく一般の有線機器であるため、管理ユニット110は、有線ネットワークへ有線機器が追加されたと認識して(ステップS1116)、電子証明書を発行せず電子証明書発行フローを終了する(ステップS1115)。
- [0048] 図7のステップS1103において、機器識別フローがエラー終了の場合は、管理ユニット110は、表示部をRランプ点灯状態に切替えて、電子証明書発行フローが異常終了したことを利用者へ通知する(ステップS1120, S1121)。
- [0049] 図7のステップS1103において、機器識別フローがネットワーク参加可能終了(OK終了)の場合は、管理ユニット110は、有線接続された新規伝送ユニット410が既に電子証明書を所有しているかどうかを確認する(図7のステップS1104、及び、図9のステップS1300〜S1310)。図9は、管理ユニット110において、有線接続された新規伝送ユニット410が既に電子証明書を所有しているかどうかを確認する電子証明書所有確認フロー(ステップS1300〜S1310)である。
- [0050] 図9のステップS1301において、管理ユニット110は、新規伝送ユニット410が電子証明書を所有しているか否かを確認する。電子証明書を所有していない場合は、管理ユニット110は、所定時間内に接続された新規伝送ユニット410からの電子証明書確認要求を受信したか否かを判定する(ステップS1302)。管理ユニット110は、所定時間内に電子証明書確認要求を受信しない場合は、電子証明書所有確認フローを終了する(ステップS1309)。ステップS1309における電子証明書所有確認フローの終了は、証明書所有確認フローを正常に終了することができなかったことを示すものであり、その結果、新規伝送ユニット410が無線ネットワーク300に参加できないので

、ネットワーク参加不可終了(図では「NG終了」と言う。

[0051] 図9のステップS1302において、管理ユニット110は、所定時間内に電子証明書確認要求を受信した場合は、電子証明書を所有していないことを示す電子証明書非所有応答を、接続された新規伝送ユニット410に対して送信し(ステップS1303)、電子証明書所有確認フローを終了する(ステップS1310)。ステップS1303及びS1310における電子証明書所有確認フローの終了は、証明書所有確認フローを正常に終了することができたことを示すものであり、その結果、新規伝送ユニット410が無線ネットワーク300において参加可能な伝送ユニットであることを示すものであり、ネットワーク参加可能終了(図では「OK終了」と言う。

[0052] 図9のステップS1301において、新規伝送ユニット410が電子証明書を所有している場合は、管理ユニット110は、接続された新規伝送ユニット410からの電子証明書確認要求を所定時間内に受信したか否かを判定する(ステップS1304)。図9のステップS1304において、所定時間内に電子証明書確認要求を受信した場合は、ステップS1308において、管理ユニット110は、電子証明書を所有していることを示す電子証明書所有応答を、接続された新規伝送ユニット410に対して送信し、電子証明書所有確認フローを終了する(ステップS1310)。ステップS1308及びS1310における電子証明書所有確認フローの終了は、証明書所有確認フローを正常に終了することができたことを示すものであり、その結果、新規伝送ユニット410が無線ネットワーク300において参加可能な伝送ユニットであることを示すものであり、ネットワーク参加可能終了(OK終了)である。

[0053] 図9のステップS1304において、管理ユニット110は、所定時間内に電子証明書確認要求を受信しなかった場合は、ステップS1305において、接続された新規伝送ユニット410に対して、電子証明書を所有しているかどうかを確認するために電子証明書確認要求を送信する。

[0054] 図9のステップS1306において、管理ユニット110は、ステップS1305において送信した電子証明書確認要求に対する電子証明書所有応答を、所定時間内に接続された新規伝送ユニット410から受信したかどうかを判定する。図9のステップS1306において、管理ユニット110は、所定時間内に電子証明書所有応答を受信しなかつ

た場合は、電子証明書所有確認フローをネットワーク参加不可終了(NG終了)する(ステップS1309)。

[0055] 図9のステップS1306において、管理ユニット110は、所定時間内に電子証明書所有応答を受信した場合には、ステップS1307において、受信した電子証明書所有応答を検証する。検証の結果、接続された新規伝送ユニット410が、管理ユニット110が所属する無線ネットワークの電子証明書と同じ電子証明書を所有していることを確認した場合は、電子証明書を発行する必要は無いため、管理ユニット110は、電子証明書所有確認フローをネットワーク参加不可終了(NG終了)する(ステップS1309)。

[0056] 図9のステップS1307において、受信した電子証明書所有応答の検証の結果、接続された新規伝送ユニット410が、電子証明書を所有していないことを確認した場合、又は、管理ユニット110が所属する無線ネットワークの電子証明書とは別のネットワークの電子証明書を所有していることを確認した場合は、管理ユニット110は、新たに電子証明書を発行するために、電子証明書所有確認フローをネットワーク参加可能終了(OK終了)する(ステップS1310)。

[0057] 図7のステップS1104において、電子証明書所有確認フローがネットワーク参加不可終了(NG終了)した場合は、管理ユニット110は、ステップS1120において、表示部をRランプ点灯状態に切替えて(ステップS1120)、電子証明書発行フローが異常終了したことを利用者へ通知する(ステップS1121)。

[0058] 図7のステップS1104において、電子証明書所有確認フローがネットワーク参加可能終了(OK終了)の場合は、図7の処理はステップS1105に進み、管理ユニット110は、新規伝送ユニット410に対して、電子証明書発行フローを開始することを示す情報を開始通知として送信する。

[0059] 図7のステップS1106において、管理ユニット110は、所定時間内に新規伝送ユニット410からの電子証明書発行要求を受信したかどうかを判定する。管理ユニット110は、所定時間内に電子証明書発行要求を受信しない場合は、処理をステップS1117～S1121のタイムアウト処理へ進める。図7のステップS1106において、新規伝送ユニット410からの応答がタイムアウトにより受信できなかった場合は、管理ユニット110は、ステップS1105の開始通知以降に受信した情報をすべてクリアする(ステッ

プS1117)。受信情報をクリアした後、管理ユニット110は、電子証明書発行フローのリトライ回数を示すリトライカウンタを更新する(ステップS1118)。管理ユニット110は、リトライカウンタを更新した後、リトライカウンタが所定回数に達したかどうかを確認する(ステップS1119)。リトライカウンタが所定回数に達していない場合は、管理ユニット110は、処理をステップS1105へ戻し、新規伝送ユニット410に対して再び開始通知を送信する。リトライカウンタが所定回数に達した場合は、管理ユニット110は、表示部をRランプ点灯状態へ切替えて(ステップS1120)、異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS1121)。

[0060] 図7のステップS1106において、所定時間内に電子証明書発行要求を受信した場合は、管理ユニット110は、表示部をRランプ点滅状態に切替えて(ステップS1107)、電子証明書発行フロー中であることを利用者へ通知する。

[0061] 図7のステップS1108において、管理ユニット110は、新規伝送ユニット410に対して、電子証明書に記載するための伝送ユニットに固有の情報を得るためにユニット情報要求を送信する。

[0062] 図7のステップS1109において、管理ユニット110は、所定時間内に新規伝送ユニット410からのユニット情報を受信したか否かを判定する。ユニット情報としては、MACアドレス等の伝送ユニット固有の機器識別子が挙げられる。管理ユニット110は、所定時間内にユニット情報を受信しない場合は、処理をステップS1117～S1121のタイムアウト処理へ進める。図7のステップS1109において、管理ユニット110は、新規伝送ユニット410からのユニット情報を受信した場合には、新規伝送ユニット410から受信したユニット情報に基づいて電子証明書を作成し発行する(ステップS1110)。

[0063] 次に、図7のステップS1111において、管理ユニット110は、発行した電子証明書を新規伝送ユニット410が受領したかどうかを示す電子証明書応答を所定時間内に受信したか否かを判定する。管理ユニット110は、所定時間内に電子証明書応答を受信しない場合は、処理をステップS1117～S1121のタイムアウト処理へ進める。図7のステップS1111において、管理ユニット110は、受信した電子証明書応答を受理していない場合は、電子証明書応答に含まれるユニット情報を基に再度電子証明書を作成し、ステップS1110へ戻り再び電子証明書を発行する。管理ユニット110は、

受信した電子証明書応答を受領した場合は、表示部を元のGランプ点灯状態へ切替え(ステップS1112)、処理を次のステップS1113へ進める。

[0064] 図7のステップS1113において、管理ユニット110は、新規伝送ユニット410に対して電子証明書発行フローの終了を示す終了通知を送信する。図7のステップS1114において、利用者は、管理ユニット110と新規伝送ユニット410の表示部を確認して有線接続を切断し、電子証明書発行フローを終了する(ステップS1115)。

[0065] 以下に、実施の形態1における新規伝送ユニット410の動作手順を詳細に説明する。図10は、管理ユニット110へ有線接続された新規伝送ユニット410において、新規伝送ユニット410が電子証明書を取得する手順を示すフロー(ステップS1400～S1423)である。

[0066] 図10に示されるように、新規伝送ユニット410は、電子証明書を所有しておらず、かつ、無線ネットワーク300へ参加していないので、表示部は無灯状態である(ステップS1401)。図10のステップS1402において、利用者は、新規伝送ユニット410と管理ユニット110を、利用者が確実に安全であると認識できる有線により接続する。

[0067] 図10のステップS1403において、有線接続された機器(新規伝送ユニット410)が、無線ネットワーク300において通信可能な通信手段を備えた伝送ユニットであるかを識別する。機器識別フローは、前述した図8のフローと同様である。

[0068] 図10のステップS1403において、機器識別フローがネットワーク参加不可終了(NG終了)の場合は、接続された機器は無線ネットワーク300において通信可能な伝送ユニットではなく一般の有線機器であるため、有線ネットワーク(例えば、図1におけるネットワーク100)へ有線機器が追加されたと認識して(ステップS1417)、電子証明書は発行されず、電子証明書発行フローを終了する(ステップS1416)。

[0069] 図10のステップS1403において、機器識別フローがエラー終了の場合は、新規伝送ユニット410は、表示部をRランプ点灯状態に切替え(ステップS1422)、電子証明書発行フローが異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS1423)。

[0070] 図10のステップS1403において、機器識別フローがネットワーク参加可能終了(OK終了)したことにより、接続された機器は無線ネットワーク300において通信可能な

伝送ユニットであると判断されたときは、次の図10のステップS1404において、有線接続された新規伝送ユニット410が既に電子証明書を所有しているかどうか、確認される。電子証明書所有確認フローについては、前述した図9のフローと同様である。

- [0071] 図10のステップS1404において、電子証明書所有確認フローがネットワーク参加不可終了(NG終了)の場合は、表示部をRランプ点灯状態に切替え(ステップS1422)、電子証明書発行フローが異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS1423)。
- [0072] 図10のステップS1405においては、電子証明書所有確認フロー(ステップS1404)がネットワーク参加可能終了(OK終了)であったため、新規伝送ユニット410は、管理ユニット110から電子証明書発行フローの開始を示す開始通知を受信する。新規伝送ユニット410は、所定時間内に開始通知を受信しない場合は、表示部をRランプ点灯状態に切替え(ステップS1422)、電子証明書発行フローが異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS1423)。図10のステップS1405において、新規伝送ユニット410は、所定時間内に開始通知を受信した場合は、表示部をRランプ点滅状態に切替え(ステップS1406)、電子証明書発行フロー中であることを利用者へ通知して電子証明書発行フローを終了する(ステップS1423)。
- [0073] 図10のステップS1407において、新規伝送ユニット410は、管理ユニット110に対して、電子証明書発行要求を送信する。図10のステップS1408において、新規伝送ユニット410は、管理ユニット110からのユニット情報要求を所定時間内に受信したか否かを判定する。新規伝送ユニット410は、所定時間内にユニット情報要求を受信しない場合は、処理をステップS1419〜S1423のタイムアウト処理へ進める。図10において、管理ユニット110からの応答がタイムアウトにより受信できなかった場合、新規伝送ユニット410は、ステップS1405の開始通知以降に受信した情報をすべてクリアする(ステップS1419)。新規伝送ユニット410は、受信情報をクリアした後、電子証明書発行フローのリトライ回数を示すリトライカウンタを更新する(ステップS1420)。新規伝送ユニット410は、リトライカウンタを更新した後、リトライカウンタが所定回

数に達したかどうかを確認する(ステップS1421)。新規伝送ユニット410は、リトライカウンタが所定回数に達していない場合は、ステップS1405へ戻り再び開始通知を受信する。新規伝送ユニット410は、リトライカウンタが所定回数に達した場合は、表示部をRランプ点灯状態へ切替え(ステップS1422)、異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS1423)。

[0074] 図10のステップS1408において、所定時間内にユニット情報要求を受信した場合には、新規伝送ユニット410は、次のステップS1409において、管理ユニット110に対して、電子証明書に記載するための伝送ユニット固有の情報をユニット情報通知として送信する。ユニット情報としては、MACアドレス等の伝送ユニットに固有の機器識別子が挙げられる。

[0075] 図10のステップS1410において、新規伝送ユニット410は、管理ユニット110から、所定時間内にユニット情報に基づいて作成された電子証明書を含む電子証明書発行を受信したか否かを判定する。新規伝送ユニット410は、所定時間内に電子証明書発行を受信しない場合は、処理をステップS1419～S1423のタイムアウト処理へ進める。

[0076] 図10のステップS1410において、新規伝送ユニット410は、所定時間内に電子証明書発行を受信した場合は、管理ユニット110から受信した電子証明書の内容を検証する(ステップS1411)。電子証明書の内容を検証した結果、発行要求とは異なる電子証明書であった場合は、新規伝送ユニット410は、管理ユニット110に対して不受理通知を送信し(ステップS1418)、処理をステップS1410へ戻して再び電子証明書発行を受信する。電子証明書の内容を検証した結果、発行要求に応じた電子証明書であった場合は、新規伝送ユニット410は、管理ユニット110に対して電子証明書発行応答を送信する(ステップS1412)。

[0077] 図10のステップS1413において、新規伝送ユニット410は、所定時間内に管理ユニット110から電子証明書発行フローの終了を示す終了通知を受信したか否かを判定する。所定時間内に終了通知を受信しない場合は、新規伝送ユニット410は、処理をステップS1419～S1423のタイムアウト処理へ進める。

[0078] 図10のステップS1413において、所定時間内に終了通知を受信した場合は、新

規伝送ユニット410は、表示部をGランプ点滅状態に切替え(ステップS1414)、電子証明書を取得したことを利用者へ通知する。利用者は表示部がGランプ点滅状態に切替わったことを確認して、管理ユニット110との有線接続を切断し(ステップS1415)、電子証明書発行フローを終了する(ステップS1416)。

[0079] 以上に説明したように、実施の形態1の電子証明書発行方法によれば、新規伝送ユニット410が電子証明書を所有しているかどうか、管理ユニット110が無線ネットワーク300に参加しているかどうか、管理ユニット110又は新規伝送ユニット410が電子証明書発行フロー中であるかどうか、管理ユニット110又は新規伝送ユニット410が処理を異常終了していないかどうかというような、伝送ユニットの状況をリアルタイムに確認しながら、電子証明書発行処理を進めることができる。

[0080] また、実施の形態1の電子証明書発行方法によれば、新規伝送ユニット410を管理ユニット110に第三者からの不正アクセスに対して利用者が確実に安全であると認識できる有線で接続するため、キーボード等によりパスフレーズを入力する必要はなく、簡単な操作で無線ネットワークへの参加に必要な電子証明書を取得することができる。

[0081] さらに、実施の形態1の電子証明書発行方法によれば、新規伝送ユニット410が無線ネットワーク300に参加できる通信手段を備えた機器であると識別したときであっても、新規伝送ユニット410が既に電子証明書を所有している場合には、電子証明書を新たに発行しないことにより、不必要な処理を省略することができる。

[0082] さらにまた、実施の形態1の電子証明書発行方法によれば、新規伝送ユニット410が無線ネットワーク300に参加できる通信手段を備えた機器であると識別し、かつ、新規伝送ユニット410が既に電子証明書を所有しているときであっても、既に所有している電子証明書が無線ネットワーク300とは別のネットワークの電子証明書である場合には、機器識別子を用いて新規伝送ユニット410用の電子証明書を作成し、作成された電子証明書を新規伝送ユニット410に送信する処理を実行するので、電子証明書を確実に発行することができる。

[0083] また、実施の形態1の電子証明書発行方法によれば、新規伝送ユニット410は、受信した電子証明書の正当性を検証し、正当性が確認された場合には、電子証明書を

発行した管理ユニット110に対して電子証明書を受領したことを通知するので、利用者は電子証明書が発行されたことを確認することができる。また、新規伝送ユニット410は、受信した電子証明書の正当性を検証し、正当性が確認されない場合には、電子証明書を発行した管理ユニット110に対して再度電子証明書の発行を要求するので、電子証明書を確実に発行することができる。

[0084] なお、上記説明においては、新規伝送ユニット410を管理ユニット110に接続した場合を説明したが、管理ユニット110が所属する有線ネットワーク内の機器(例えば、図1の機器120)であれば、管理ユニット110以外の有線機器に接続してもよい。

[0085] また、上記説明においては、新規伝送ユニット410は、管理ユニット110が所属する無線ネットワークの電子証明書を既に所有している場合には、電子証明書発行フローを実行せず終了する例を示したが、既に電子証明書を所有している場合であっても、電子証明書発行フローを実行して、電子証明書を発行してもよい。

[0086] 実施の形態2.

上記実施の形態1においては、新規伝送ユニット410を、電子証明書を発行する管理ユニット110に有線接続した場合を説明したが、実施の形態2においては、新規伝送ユニット410を、電子証明書を発行する管理ユニット110が参加する無線ネットワーク300に参加している他の伝送ユニット210に有線接続した場合を説明する。

[0087] 図11は、本発明の実施の形態2に係る電子証明書発行方法を説明するための構成図である。図11において、図1又は図5(実施の形態1)の構成と同一又は対応する構成には同じ符号を付す。また、図11に示される各伝送ユニット110, 210, 410の構成は、上記実施の形態1において説明した構成(図2〜図4)と同様である。

[0088] 最初に、図11を用いて、無線ネットワーク300への参加権限を証明する電子証明書を所有していない新規伝送ユニット410が、管理ユニット110から伝送ユニット210を経由して無線ネットワーク300への参加権限を証明する電子証明書416の発行を受けるための動作の概略を説明する。なお、実施の形態2の説明に際しては、図2〜図4をも参照する。

[0089] まず、利用者は、新規伝送ユニット410の有線通信部412と、伝送ユニット210の有線通信部212とを、例えば、IEEE1394規格に準拠した通信ケーブルによって、

接続する。利用者は、新規伝送ユニット410の有線通信部412と、伝送ユニット210の有線通信部212とを、通信ケーブルによって直接接続することによって、新規伝送ユニット410と伝送ユニット210とを、悪意ある第三者からの不正アクセスに対して、利用者が明らかに安全であると認識することができる。また、伝送ユニット210と管理ユニット110とは、互いに電子証明書を交換して通信することによって、悪意ある第三者からの不正アクセスに対するセキュリティを確保することができる。

[0090] 新規伝送ユニット410が接続された後、伝送ユニット210は、新規伝送ユニット410の機器種別情報を受信する。伝送ユニット210は、新規伝送ユニット410の機器種別情報に基づいて、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた機器であるか否かを識別する。なお、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた機器であるか否かの識別は、伝送ユニット210ではなく、管理ユニット110が行ってもよい。また、管理ユニット110は、伝送ユニット210を経由して、新規伝送ユニット410に固有の機器情報である機器識別子(ユニット情報)を受信する。

[0091] 管理ユニット110は、新規伝送ユニット410が無線ネットワーク300において通信可能な通信手段を備えた機器であると識別した場合に、新規伝送ユニット410の機器識別子を用いて電子証明書416を作成し、作成された電子証明書416を伝送ユニット210を経由して、新規伝送ユニット410に送信する。以上により、管理ユニット110による、新規伝送ユニット410に対する電子証明書416の発行処理が終了する。

[0092] 図12は、実施の形態2に係る電子証明書発行方法の手順を示す図である。以下に、図12に基づいて、新規伝送ユニット410を、伝送ユニット210に接続し、管理ユニット110から電子証明書の発行を受けるときの電子証明書授受動作について説明する。図12において、管理ユニット110、伝送ユニット210、及び新規伝送ユニット410は、現在の伝送ユニットの状況を利用者へ通知するための表示部を備えており、表示部のGランプ及びRランプ表示状態の意味は実施の形態1の場合と同じである。また、図12において、実線矢印で示されるフローは有線通信であることを示し、破線矢印で示されるフローは無線通信であることを示している。

[0093] 図12のステップS2000において、利用者は、伝送ユニット210と新規伝送ユニット

410を有線で接続する。このとき、伝送ユニット210は、電子証明書を所有しており、かつ、無線ネットワーク300へ参加しているので、伝送ユニット210の表示部はGランプ点灯状態である。一方、新規伝送ユニット410は電子証明書を所有しておらず、かつ、無線ネットワーク300へ参加していないので、新規伝送ユニット410の表示部はランプ無灯状態である。また、管理ユニット110は、電子証明書を所有しており、かつ、無線ネットワーク300へ参加しているので、管理ユニット110の表示部はGランプ点灯状態である。

- [0094] 図12のステップS2001において、有線接続された機器(新規伝送ユニット410)が、無線ネットワーク300において通信可能な通信手段を備えた伝送ユニットであるかを識別する機器識別をする。機器識別ステップの詳細は、実施の形態1における図8で示す処理フローと同様である。図12には、この機器識別ステップを伝送ユニット210が行う場合が示されているが、このステップを管理ユニット110が行ってもよい。
- [0095] 図12のステップS2002において、有線接続された新規伝送ユニット410が既に電子証明書を所有しているか否かを確認する電子証明書所有確認を実行する。電子証明書所有確認ステップの詳細は、実施の形態1における図9で示す処理フローと同様である。図12には、この電子証明書所有確認ステップを伝送ユニット210が行う場合が示されているが、このステップを管理ユニット110が行ってもよい。
- [0096] 図12のステップS2003において、伝送ユニット210は、新規伝送ユニット410に対して、電子証明書発行フローの開始を通知する開始通知を送信し、タイマ1を起動する。開始通知を受信した新規伝送ユニット410は、表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知する。新規伝送ユニット410は、次のステップS2004において、伝送ユニット210に対して電子証明書発行要求Aを送信し、タイマ2を起動する。電子証明書発行要求Aを受信した伝送ユニット210は、表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知し、タイマ1を終了する。伝送ユニット210は、タイマ1がタイムアウトする前に、電子証明書発行要求Aを受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。

- [0097] 図12のステップS2004において、タイマ1がタイムアウトする前に電子証明書発行要求Aを受信した伝送ユニット210は、電子証明書を発行することができないので、次のステップS2005において、管理ユニット110に対して電子証明書発行要求Bを無線ネットワーク300による無線通信により送信し、タイマ3を起動する。電子証明書発行要求Bを受信した管理ユニット110は、表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知する。
- [0098] 図12のステップS2005において、電子証明書発行要求を受信した管理ユニット110は、次のステップS2006において、電子証明書に記載するためのユニット情報を得るために、伝送ユニット210に対して、無線通信によりユニット情報要求Aを送信しタイマ4を起動する。ユニット情報要求Aを受信した伝送ユニット210は、タイマ3を終了する。伝送ユニット210は、タイマ3がタイムアウトする前に、ユニット情報要求Aを受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。
- [0099] 図12のステップS2006において、タイマ3がタイムアウトする前にユニット情報要求を受信した伝送ユニット210は、次のステップS2007において、新規伝送ユニット410に対してユニット情報要求Bを有線通信により送信し、タイマ5を起動する。ユニット情報要求Bを受信した新規伝送ユニット410は、タイマ2を終了する。新規伝送ユニット410は、タイマ2がタイムアウトする前にユニット情報要求Bを受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。
- [0100] 図12のステップS2007において、タイマ2がタイムアウトする前にユニット情報要求Bを受信した新規伝送ユニット410は、次のステップS2008において、伝送ユニット210に対してユニット情報通知Aを有線通信により送信し、タイマ6を起動する。ユニット情報通知Aを受信した伝送ユニット210は、タイマ5を終了する。伝送ユニット210は、タイマ5がタイムアウトする前にユニット情報通知Aを受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。
- [0101] 図12のステップS2008において、タイマ5がタイムアウトする前にユニット情報通知

Aを受信した伝送ユニット210は、次のステップS2009において、管理ユニット110に対してユニット情報通知Bを無線ネットワーク300による無線通信により送信し、タイマ7を起動する。ユニット情報通知Bを受信した管理ユニット110は、タイマ4を終了する。管理ユニット110は、タイマ4がタイムアウトする前にユニット情報通知Bを受信しなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図13のステップS2111〜S2110)。

[0102] 図12のステップS2009において、タイマ4がタイムアウトする前にユニット情報通知Bを受信した管理ユニット110は、受信したユニット情報を基に電子証明書を作成し、次のステップS2010において、伝送ユニット210に対して電子証明書発行Aを無線ネットワーク300による無線通信により送信し、タイマ8を起動する。電子証明書発行Aを受信した伝送ユニット210は、タイマ7を終了する。伝送ユニット210は、タイマ7がタイムアウトする前に電子証明書発行Aを受信できなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。

[0103] 図12のステップS2010において、タイマ7がタイムアウトする前に電子証明書発行Aを受信した伝送ユニット210は、次のステップS2011において、新規伝送ユニット410に対して電子証明書発行Bを有線通信により送信し、タイマ9を起動する。電子証明書発行Bを受信した新規伝送ユニット410は、タイマ6を終了する。新規伝送ユニット410は、タイマ6がタイムアウトする前に電子証明書発行Bを受信できなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。

[0104] 図12のステップS2011において、タイマ6がタイムアウトする前に電子証明書発行Bを受信した新規伝送ユニット410は、受信した電子証明書の内容を検証し、電子証明書の正当性を確認した場合には、次のステップS2012において伝送ユニット210に対して、電子証明書を正常に受領したことを通知する電子証明書発行応答Aを送信し、タイマ10を起動する。新規伝送ユニット410は、電子証明書の内容が不当である場合には、電子証明書発行応答Aに再度ユニット情報を含めて送信する。電子証明書発行応答Aを受信した伝送ユニット210は、タイマ9を終了する。伝送ユニット21

0は、タイマ9がタイムアウトする前に電子証明書発行応答Aを受信できなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。

[0105] 図12のステップS2012において、タイマ9がタイムアウトする前に電子証明書発行応答Aを受信した伝送ユニット210は、次のステップS2013において、管理ユニット110に対して電子証明書発行応答Bを無線ネットワーク200による無線通信により送信し、タイマ11を起動する。電子証明書発行応答Bを受信した管理ユニット110は、表示部を元のGランプ点灯状態に戻し、タイマ8を終了する。タイマ8がタイムアウトする前に電子証明書発行応答Bを受信できなかった場合には、管理ユニット110は、タイムアウト処理を実行する。タイムアウト処理については後述する(図13のステップS2111〜S2110)。

[0106] 図12のステップS2013において、タイマ8がタイムアウトする前に電子証明書発行応答Bを受信した管理ユニット110は、発行した電子証明書の正当性が確認された場合には、次のステップS2014において、伝送ユニット210に対して電子証明書発行フローを終了させる終了通知Aを送信する。終了通知Aを受信した伝送ユニット210は、表示部を元のGランプ点灯状態に戻し、タイマ11を終了する。伝送ユニット210は、タイマ11がタイムアウトする前に終了通知Aを受信できなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。ステップS2013において、電子証明書発行応答Bを受信した管理ユニット110は、発行した電子証明書が不当である場合には、受信した電子証明書発行応答Bに含まれるユニット情報を基に再度電子証明書を作成し、処理をステップS2010へ戻し、新規伝送ユニット410に対して再度電子証明書を発行する。

[0107] 図12のステップS2014において、タイマ11がタイムアウトする前に終了通知Aを受信した伝送ユニット210は、次のステップS2015において、新規伝送ユニット410に対して終了通知Bを有線通信により送信する。終了通知Bを受信した新規伝送ユニット410は、タイマ10を終了する。新規伝送ユニット410は、タイマ10がタイムアウトする前に終了通知Bを受信できなかった場合には、タイムアウト処理を実行する。タイムアウト処理については後述する(図15のステップS2224〜S2228)。

- [0108] 図12のステップS2015において、タイマ10がタイムアウトする前に終了通知Bを受信した新規伝送ユニット410は、表示部をGランプ点滅状態に切替えて、電子証明書発行フローが正常に終了して電子証明書が取得できたことを利用者へ通知する。利用者はGランプ点滅状態を確認して、ステップS2016において、有線接続を切断することができる。以上のフローにより、新規伝送ユニット410は、管理ユニット110から伝送ユニット210を経由して、無線ネットワーク300へ参加するための電子証明書を取得することができる。
- [0109] 次に、実施の形態2において、管理ユニット110における詳細な動作手順を説明する。図13は、実施の形態2に係る電子証明書発行方法における管理ユニット110の動作を示すフローチャートである。具体的にいえば、図13は、図12で示すフローにおける伝送ユニット210へ有線接続された新規伝送ユニット410に対して、管理ユニット110が電子証明書を発行する手順を示すフロー（ステップS2100〜S2111）である。
- [0110] 図13に示されるように、管理ユニット110は電子証明書を所有しており、かつ、無線ネットワークへ参加しているので表示部はGランプ点灯状態である（ステップS2101）。
- [0111] 図13のステップS2102において、管理ユニット110は、伝送ユニット210から電子証明書発行要求Bを受信した場合は、ステップS2103において、管理ユニット110の表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知する。
- [0112] 図13のステップS2104において、管理ユニット110は、伝送ユニット210に対して、電子証明書に記載するためのユニット固有の情報を得るためにユニット情報要求Aを送信する。
- [0113] 図13のステップS2105において、管理ユニット110は、伝送ユニット210からユニット情報通知Bを受信する。管理ユニット110は、所定時間内にユニット情報通知Bを受信できなかった場合は、ステップS2111において、電子証明書発行フロー中に受信した情報をクリアした後、ステップS2112において、表示部を基のGランプ点灯状態へ戻し、電子証明書発行フローを終了する（ステップS2110）。

- [0114] 図13のステップS2106において、管理ユニット110は、伝送ユニット210から受信したユニット情報に基づいて電子証明書を作成し、電子証明書発行Aを送信する。
- [0115] 図13のステップS2107において、管理ユニット110は、発行した電子証明書を新規伝送ユニット410が受領したかどうかを示す電子証明書応答Bを受信する。管理ユニット110は、所定時間内に電子証明書応答Bを受信しない場合は、ステップS2111において、電子証明書発行フロー中に受信した情報をクリアした後、ステップS2112において、表示部を基のGランプ点灯状態へ戻し、電子証明書発行フローを終了する(ステップS2110)。
- [0116] 図13のステップS2107において、所定時間内に電子証明書応答Bを受信した管理ユニット110は、受信した電子証明書応答が不受理の場合は、電子証明書応答Bに含まれるユニット情報を基に再度電子証明書を作成し、処理をステップS2106へ戻し、再び電子証明書を発行する。管理ユニット110は、受信した電子証明書応答Bが受領の場合は、ステップS2108において、表示部を元のGランプ点灯状態へ切替える。
- [0117] 図13のステップS2109において、管理ユニット110は、伝送ユニット210に対して電子証明書発行フローの終了を示す終了通知を送信し、電子証明書発行フローを終了する(ステップS2110)。
- [0118] 次に、実施の形態2において、伝送ユニット210における詳細な動作手順を説明する。図14及び図15は、実施の形態2に係る電子証明書発行方法における中継用の伝送ユニットの動作を示すフローチャートである。具体的には、図14及び図15は、図12で示すフローにおける管理ユニット110へ有線接続された新規伝送ユニット410において、伝送ユニット210が、管理ユニット110と新規伝送ユニット410との間の電子証明書発行フローを中継する手順を示すフロー(ステップS2200〜S2228)である。
- [0119] 図14において、伝送ユニット210は、電子証明書を所有しており、かつ、無線ネットワーク300へ参加しているので、伝送ユニット210の表示部はGランプ点灯状態である(ステップS2201)。
- [0120] 図14のステップS2202において、伝送ユニット210と新規伝送ユニット410を、利

用者がネットワークセキュリティ上確実に安全であると認識できる有線により接続する。
。

- [0121] 図14のステップS2203において、伝送ユニット210は、有線接続された機器(新規伝送ユニット410)が無線ネットワーク300において通信可能な通信手段を備えた伝送ユニットであるか否かを識別する。なお、この機器識別フローは、伝送ユニット210以外の無線ネットワーク300に参加している伝送ユニット(例えば、管理ユニット110)が行ってもよい。機器識別フローの内容は、実施の形態1における図8で示すフローと同様である。
- [0122] 図14のステップS2203において、機器識別フローがネットワーク参加不可終了(NG終了)の場合は、接続された機器は無線ネットワーク300における通信が可能な伝送ユニットではなく一般の有線機器であるため、ステップS2222において、有線ネットワークへ有線機器が追加されたと認識して、電子証明書を発行せず電子証明書発行フローを終了する(図15のステップS2221)。
- [0123] 図14のステップS2203において、機器識別フローがエラー終了の場合は、伝送ユニット210は、ステップS2227において、表示部をRランプ点灯状態に切替えて電子証明書発行フローが異常終了したことを利用者へ通知し、電子証明書発行フローを終了する(図15のステップS2228)。
- [0124] 図14のステップS2204においては、伝送ユニット210は、ステップS2203における機器識別フローがネットワーク参加可能終了(OK終了)したことにより、接続された機器は伝送ユニットであると判断されたため、次に有線接続された新規伝送ユニット410が既に電子証明書を所有しているかどうかを確認する。なお、この電子証明書所有識別フローは、伝送ユニット210以外の無線ネットワーク300に参加している伝送ユニット(例えば、管理ユニット110)が行ってもよい。電子証明書所有確認フローの内容は、前述した図9のフローと同様である。
- [0125] 図14のステップS2204において、電子証明書所有確認フローがネットワーク参加不可終了(NG終了)の場合は、ステップS2227において、伝送ユニット210は、表示部をRランプ点灯状態に切替えて電子証明書発行フローが異常終了したことを利用者へ通知して電子証明書発行フローを終了する(図15のステップS2228)。

- [0126] 図14のステップS2205において、伝送ユニット210は、新規伝送ユニット410に対して、電子証明書発行フローを開始することを示す開始通知を送信する。
- [0127] 図14のステップS2206において、伝送ユニット210は、新規伝送ユニット410からの電子証明書発行要求Aを受信する。伝送ユニット210は、所定時間内に電子証明書発行要求Aを受信しない場合は、図15のステップS2224～S2228のタイムアウト処理を実行する。図14において、新規伝送ユニット410及び管理ユニット110からの応答がタイムアウトにより受信できなかった場合は、伝送ユニット210は、ステップS2205以降に受信した情報をすべてクリアする(ステップS2224)。伝送ユニット210は、受信情報をクリアした後、電子証明書発行フローのリトライ回数を示すリトライカウンタを更新する(ステップS2225)。伝送ユニット210は、リトライカウンタを更新した後、リトライカウンタが所定回数に達したかどうかを確認する(ステップS2226)。所伝送ユニット210は、所定回数に達していない場合は、処理をステップS2205へ戻し、新規伝送ユニット410に対して再び開始通知を送信する。伝送ユニット210は、所定の回数に達した場合は、表示部をRランプ点灯状態へ切替え(ステップS2227)、異常終了したことを利用者へ通知して電子証明書発行フローを終了する(ステップS2228)。
- [0128] 図14のステップS2206において、伝送ユニット210は、所定時間内に電子証明書発行要求Aを受信した場合は、ステップS2207において、表示部をRランプ点滅状態に切替えて電子証明書発行フロー中であることを利用者へ通知する。
- [0129] 図14のステップS2208において、伝送ユニット210は、新規伝送ユニット410から有線で受信した電子証明書発行要求Aを、管理ユニット110に対して無線ネットワーク300による無線で電子証明書発行要求Bとして送信する。
- [0130] 図14のステップS2209において、伝送ユニット210は、管理ユニット110からのユニット情報要求Aを、所定時間内に無線ネットワーク300による無線で受信できたかどうかを判定する。伝送ユニット210は、所定時間内にユニット情報要求Aを受信しない場合は、図15のステップS2224～S2228のタイムアウト処理を実行する。
- [0131] 図14のステップS2210において、伝送ユニット210は、管理ユニット110から無線ネットワーク300による無線で受信したユニット情報要求を、新規伝送ユニット410に

対して有線で送信する。

[0132] 図14のステップS2211において、伝送ユニット210は、新規伝送ユニット410からのユニット情報Aを有線で受信する。伝送ユニット210は、所定時間内にユニット情報Aを受信しない場合は、図15のステップS2224〜S2228のタイムアウト処理を実行する。

[0133] 図14のステップS2212において、伝送ユニット210は、新規伝送ユニット410から有線で受信したユニット情報を、管理ユニット110に対して無線ネットワーク300による無線で送信する。

[0134] 図15のステップS2213において、伝送ユニット210は、管理ユニット110からの電子証明書発行Aを所定時間内に無線ネットワーク300による無線で受信したか否かを判定する。伝送ユニット210は、所定時間内に電子証明書発行Aを受信しない場合は、ステップS2224〜S2228のタイムアウト処理を実行する。

[0135] 図15のステップS2214において、伝送ユニット210は、管理ユニット110から無線ネットワーク300による無線で受信した電子証明書発行を、新規伝送ユニット410に対して有線で送信する。

[0136] 図15のステップS2215において、伝送ユニット210は、新規伝送ユニット410からの電子証明書応答Aを所定時間内に有線で受信したか否かを判定する。伝送ユニット210は、所定時間内に電子証明書応答Aを受信しない場合は、ステップS2224〜S2228のタイムアウト処理を実行する。

[0137] 図15のステップS2215において、所定時間内に電子証明書応答Aを受信した伝送ユニット210は、受信した電子証明書応答が不受理の場合は、ステップS2223において、新規伝送ユニット410から有線で受信した不受理通知を管理ユニット110に対して無線ネットワーク300による無線で送信した後、処理をステップS2213へ戻し、再び電子証明書発行Aを無線ネットワーク300による無線で受信する。伝送ユニット210は、受信した電子証明書応答Aが受領の場合は、次のステップS2216において、新規伝送ユニット410から有線で受信した電子証明書応答を、管理ユニット110に対して無線ネットワーク300による無線で送信する。

[0138] 図15のステップS2217において、伝送ユニット210は、管理ユニット110からの終

了通知Aを所定時間内に無線ネットワーク300による無線で受信したか否かを判定する。伝送ユニット210は、所定時間内に終了通知Aを受信しない場合は、ステップS2224〜S2228のタイムアウト処理を実行する。

- [0139] 図15のステップS2218において、伝送ユニット210は、管理ユニット110から無線ネットワーク300による無線で受信した終了通知を、新規伝送ユニット410に対して有線で送信した後、ステップS2219において、表示部を元のGランプ点灯状態に切替えて電子証明書発行フローが正常に終了したことを利用者へ通知する。利用者は表示部がGランプ点灯状態に切替わったことを確認して、ステップS2220において、伝送ユニット210との有線接続を切断し電子証明書発行フローを終了する(ステップS2221)。
- [0140] 実施の形態2において、新規伝送ユニット410における詳細な動作手順は、実施の形態1における図10で示すフローと同様である。
- [0141] 以上に説明したように、実施の形態2の電子証明書発行方法によれば、新規伝送ユニット410が電子証明書を所有しているかどうか、管理ユニット110及び伝送ユニット210が無線ネットワーク300に参加しているかどうか、管理ユニット110、伝送ユニット210又は新規伝送ユニット410が電子証明書発行フロー中であるかどうか、管理ユニット110、伝送ユニット210又は新規伝送ユニット410が処理を異常終了していないかどうかというような、伝送ユニットの状況をリアルタイムに確認しながら、電子証明書発行処理を進めることができる。
- [0142] また、実施の形態2の電子証明書発行方法によれば、新規伝送ユニット410を伝送ユニット210に第三者からの不正アクセスに対して利用者が確実に安全であると認識できる有線で接続し、また、伝送ユニット210と管理ユニット110とはセキュリティが確保された無線ネットワークで接続されているため、キーボード等によりパスフレーズを入力する必要はなく、簡単な操作で無線ネットワークへの参加に必要な電子証明書を取得することができる。
- [0143] さらに、実施の形態2の電子証明書発行方法によれば、新規伝送ユニット410が無線ネットワーク300に参加できる通信手段を備えた機器であると識別したときであっても、新規伝送ユニット410が既に電子証明書を所有している場合には、電子証明書

を新たに発行しないことにより、不必要な処理を省略することができる。

[0144] さらにまた、実施の形態2の電子証明書発行方法によれば、新規伝送ユニット410が無線ネットワーク300に参加できる通信手段を備えた機器であると識別し、かつ、新規伝送ユニット410が既に電子証明書を所有しているときであっても、既に所有している電子証明書が無線ネットワーク300とは別のネットワークの電子証明書である場合には、機器識別子を用いて新規伝送ユニット410用の電子証明書を作成し、作成された電子証明書を新規伝送ユニット410に送信する処理を実行するので、電子証明書を確実に発行することができる。

[0145] また、実施の形態2の電子証明書発行方法によれば、新規伝送ユニット410は、受信した電子証明書の正当性を検証し、正当性が確認された場合には、電子証明書を発行した管理ユニット110に対して電子証明書を受領したことを通知するので、利用者は電子証明書が発行されたことを確認することができる。また、新規伝送ユニット410は、受信した電子証明書の正当性を検証し、正当性が確認されない場合には、電子証明書を発行した管理ユニット110に対して再度電子証明書の発行を要求するので、電子証明書を確実に発行することができる。

[0146] なお、上記説明においては、新規伝送ユニット410を伝送ユニット210に接続した場合を説明したが、伝送ユニット210が所属する有線ネットワーク内の機器（例えば、図1の機器220, 230）であれば、伝送ユニット210以外の有線機器に接続してもよい。

[0147] また、上記説明においては、新規伝送ユニット410は、管理ユニット110が所属する無線ネットワークの電子証明書を既に所有している場合には、電子証明書発行フローを実行せず終了する例を示したが、既に電子証明書を所有している場合であっても、電子証明書発行フローを実行して、電子証明書を発行してもよい。

[0148] 変形例の説明。

上記実施の形態1及び2においては、外部からの不正アクセスに対してセキュリティが確保されていないネットワークがIEEE802. 11規格等に準拠した無線ネットワークである場合を説明したが、本発明の電子証明書発行方法は、例えば、超広帯域無線（UWB）ネットワークやブルートゥース（Bluetooth）を用いたネットワークのような他の

無線ネットワークにも適用可能である。また、本発明の電子証明書発行方法が適用されるネットワークは、無線ネットワークに限定されるものではなく、例えば、電灯線を用いた有線ネットワークである電力線通信(PLC)ネットワークや、イーサネット(Ethernet)等に適用することもできる。

- [0149] また、実施の形態1及び2においては、外部からの不正アクセスに対して利用者が明らかに安全であると認識できるネットワークがIEEE1394規格等に準拠した有線ネットワークである場合を説明したが、有線ネットワークに限定されるものではなく、例えば、外部からの不正アクセスに対して利用者が明らかに安全であると認識できるネットワークとして赤外線を用いた無線ネットワーク(IrDA (InfraRed Data Association) 等)を用いることもできる。

請求の範囲

- [1] ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行するデータ送受信装置であって、
- 前記ネットワークにおける通信を行う第1の通信部と、
- 前記新規データ送受信装置を接続することができる第2の通信部と、
- 前記電子証明書の発行処理を行う制御部とを有し、
- 前記制御部は、
- 前記新規データ送受信装置が前記第2の通信部に接続されたときに、前記新規データ送受信装置から前記第2の通信部を経由して受信した前記新規データ送受信装置の機器種別情報に基づいて、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であるか否かを識別し、
- 前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であると識別した場合に、前記新規データ送受信装置から前記第2の通信部を経由して受信した前記新規データ送受信装置に固有の機器識別子を用いて、前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記第2の通信部を経由して前記新規データ送受信装置に送信するように制御する
- ことを特徴とするデータ送受信装置。
- [2] 前記制御部は、前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別したときであっても、前記新規データ送受信装置が既に電子証明書を所有している場合には、電子証明書を新たに発行しないことを特徴とする請求項1に記載のデータ送受信装置。
- [3] 前記制御部は、前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別し、前記新規データ送受信装置が既に電子証明書を所有しているときであっても、前記既に所有している電子証明書が前記ネットワークとは別のネットワークの電子証明書である場合には、前記機器識別子を用いて前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記

新規データ送受信装置に送信する処理を実行することを特徴とする請求項1に記載のデータ送受信装置。

- [4] ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行するデータ送受信装置であって、
前記ネットワークにおける通信を行う通信部と、
前記電子証明書の発行処理を行う制御部とを有し、
前記制御部は、
前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器である場合には、前記新規データ送受信装置から、前記新規データ送受信装置が接続されたデータ送受信装置及び前記通信部を経由して受信した前記新規データ送受信装置に固有の機器識別子を用いて、前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記通信部及び前記新規データ送受信装置が接続されたデータ送受信装置を経由して前記新規データ送受信装置に送信するように制御することを特徴とするデータ送受信装置。
- [5] 前記制御部は、前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別したときであっても、前記新規データ送受信装置が既に電子証明書を所有している場合には、電子証明書を新たに発行しないことを特徴とする請求項4に記載のデータ送受信装置。
- [6] 前記制御部は、前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別し、前記新規データ送受信装置が既に電子証明書を所有しているときであっても、前記既に所有している電子証明書が前記ネットワークとは別のネットワークの電子証明書である場合には、前記機器識別子を用いて前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記新規データ送受信装置に送信する処理を実行することを特徴とする請求項4に記載のデータ送受信装置。
- [7] ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構

成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行する電子証明書発行方法であって、

前記ネットワークを構成するデータ送受信装置の一つであって、前記新規データ送受信装置が接続されたデータ送受信装置が、

前記新規データ送受信装置から受信した前記新規データ送受信装置の機器種別情報に基づいて、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であるか否かを識別し、

前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であると識別した場合に、前記新規データ送受信装置から受信した前記新規データ送受信装置に固有の機器識別子を用いて、前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記新規データ送受信装置に送信する

ことを特徴とする電子証明書発行方法。

- [8] 前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別したときであっても、前記新規データ送受信装置が既に電子証明書を所有している場合には、電子証明書を新たに発行しないことを特徴とする請求項7に記載の電子証明書発行方法。

- [9] 前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別し、前記新規データ送受信装置が既に電子証明書を所有しているときであっても、前記既に所有している電子証明書が前記ネットワークとは別のネットワークの電子証明書である場合には、前記機器識別子を用いて前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記新規データ送受信装置に送信する処理を実行することを特徴とする請求項7に記載の電子証明書発行方法。

- [10] 前記新規データ送受信装置は、受信した前記電子証明書の正当性を検証し、正当性が確認された場合には、前記電子証明書を発行したデータ送受信装置に対して前記電子証明書を受領したことを通知し、正当性が確認されない場合には、前記電子証明書を発行したデータ送受信装置に対して再度電子証明書の発行を要求す

ることを特徴とする請求項7に記載の電子証明書発行方法。

- [11] ネットワーク参加権限を証明する電子証明書を所有するデータ送受信装置から構成されるネットワークに、新規データ送受信装置を参加させる際に、前記新規データ送受信装置に対して電子証明書を発行する電子証明書発行方法であって、

前記ネットワークを構成するデータ送受信装置の一つが、前記新規データ送受信装置から、前記新規データ送受信装置が接続されたデータ送受信装置を経由して受信した前記新規データ送受信装置の機器種別情報に基づいて、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であるか否かを識別し、

前記ネットワークを構成するデータ送受信装置の一つであって、前記新規データ送受信装置が接続されたデータ送受信装置以外のデータ送受信装置が、前記新規データ送受信装置が前記ネットワークにおいて通信可能な通信手段を備えた機器であると識別した場合に、前記新規データ送受信装置から、前記新規データ送受信装置が接続されたデータ送受信装置を経由して受信した前記新規データ送受信装置に固有の機器識別子を用いて、前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記新規データ送受信装置が接続されたデータ送受信装置を経由して前記新規データ送受信装置に送信する

ことを特徴とする電子証明書発行方法。

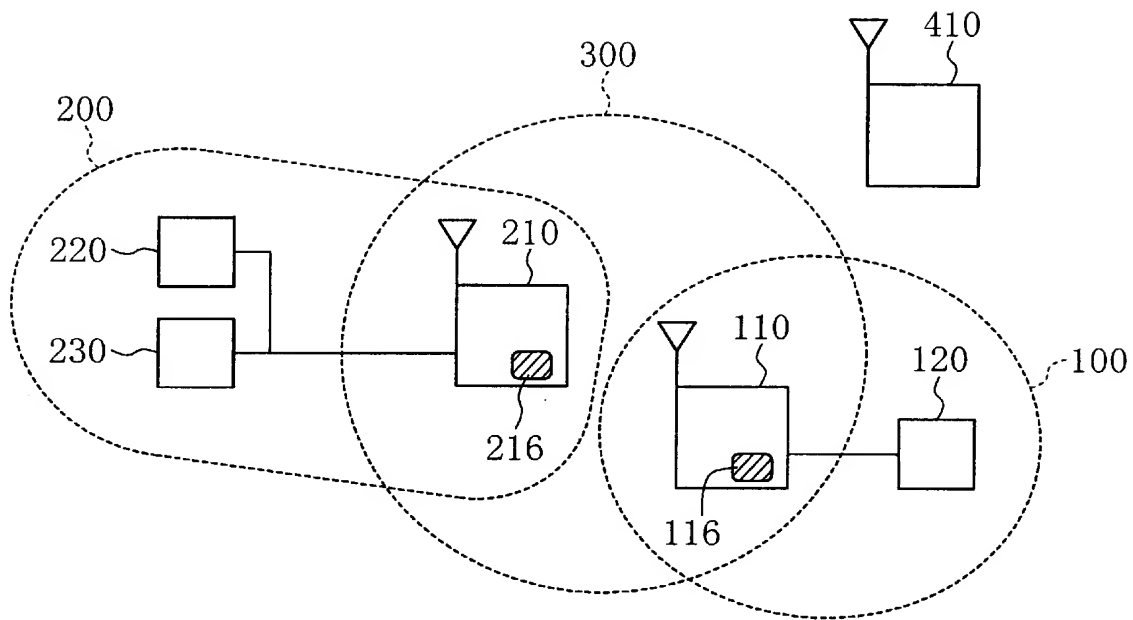
- [12] 前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別したときであっても、前記新規データ送受信装置が既に電子証明書を所有している場合には、電子証明書を新たに発行しないことを特徴とする請求項11に記載の電子証明書発行方法。

- [13] 前記新規データ送受信装置が前記ネットワークに参加できる通信手段を備えた機器であると識別し、前記新規データ送受信装置が既に電子証明書を所有しているときであっても、前記既に所有している電子証明書が前記ネットワークとは別のネットワークの電子証明書である場合には、前記機器識別子を用いて前記新規データ送受信装置用の電子証明書を作成し、前記作成された電子証明書を前記新規データ送受信装置に送信する処理を実行することを特徴とする請求項11に記載の電子証明

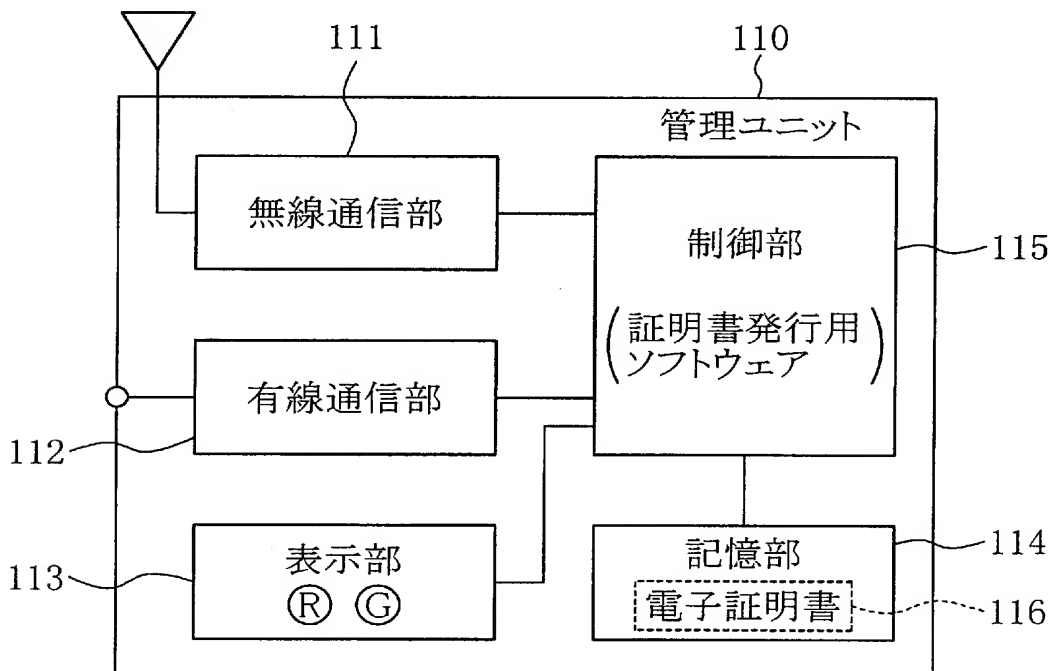
書発行方法。

- [14] 前記新規データ送受信装置は、受信した前記電子証明書の正当性を検証し、正当性が確認された場合には、前記電子証明書を発行したデータ送受信装置に対して前記電子証明書を受領したことを通知し、正当性が確認されない場合には、前記電子証明書を発行したデータ送受信装置に対して再度電子証明書の発行を要求することを特徴とする請求項11に記載の電子証明書発行方法。

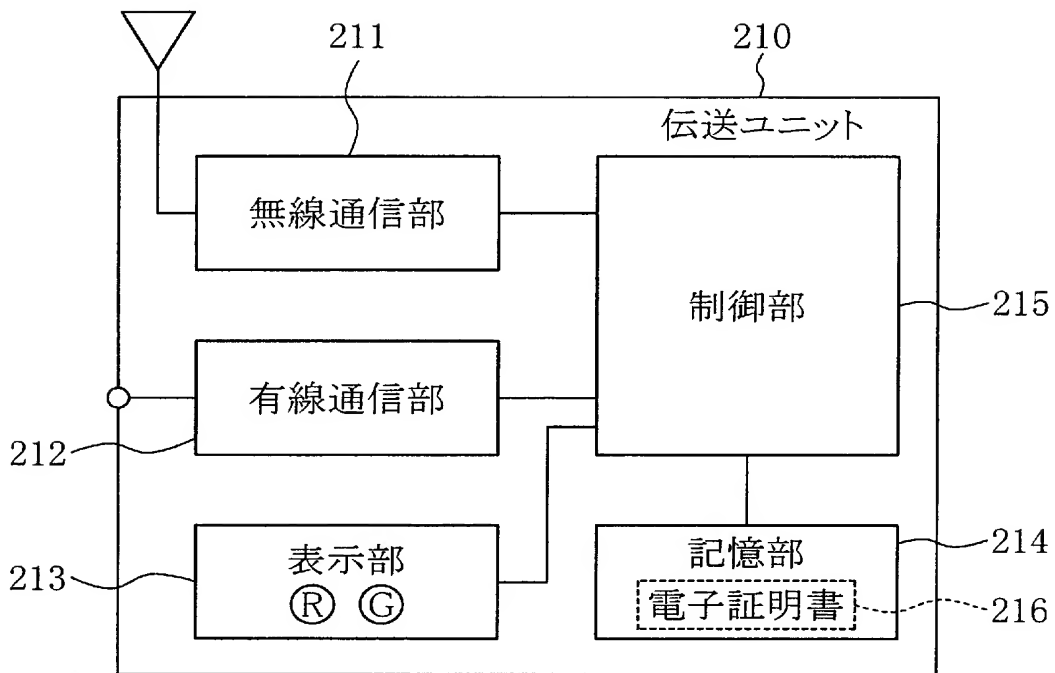
[図1]



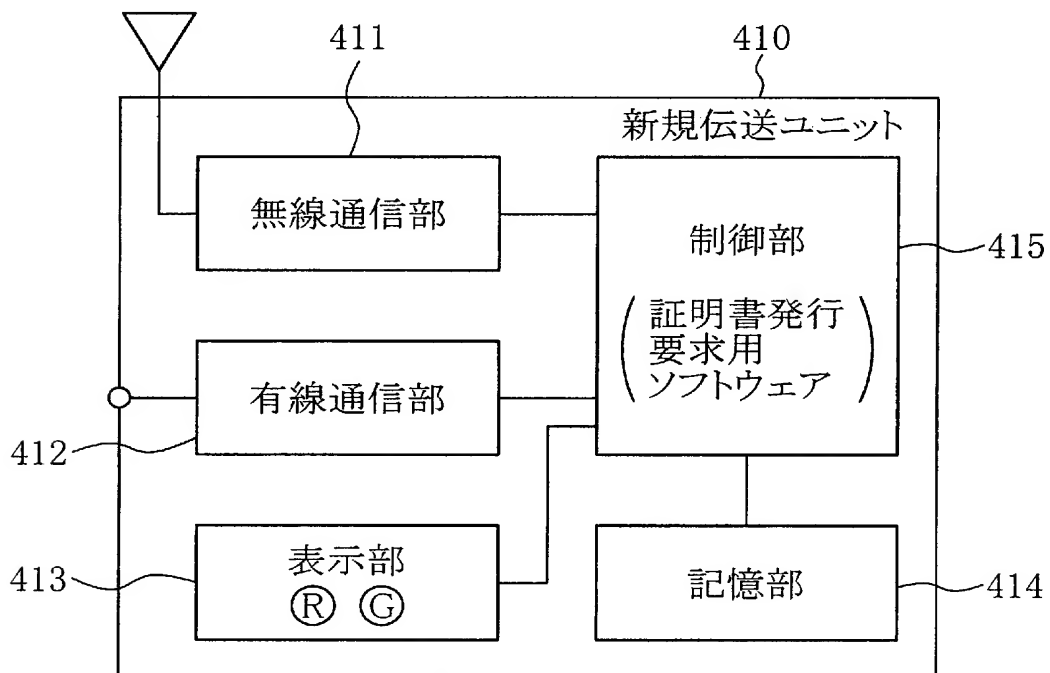
[図2]



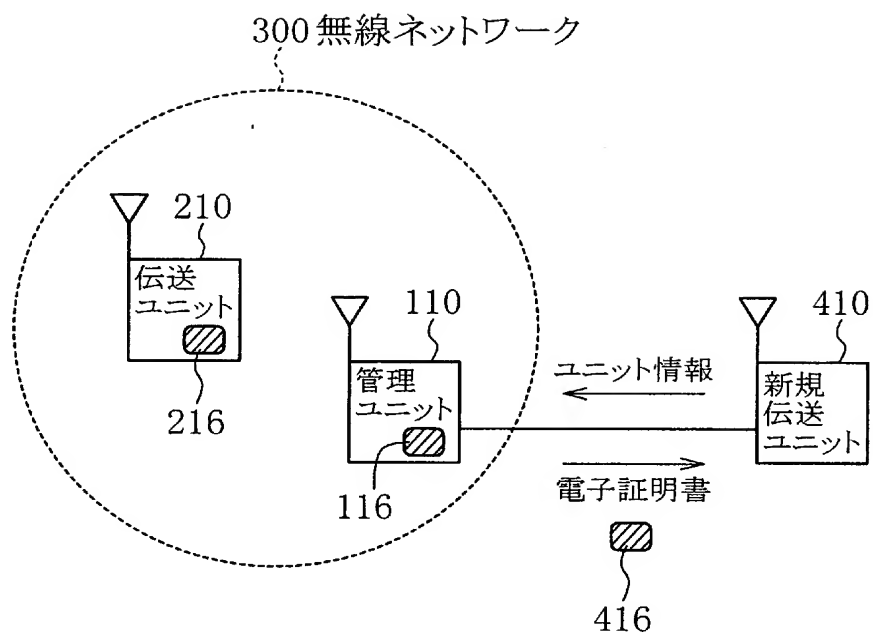
[図3]



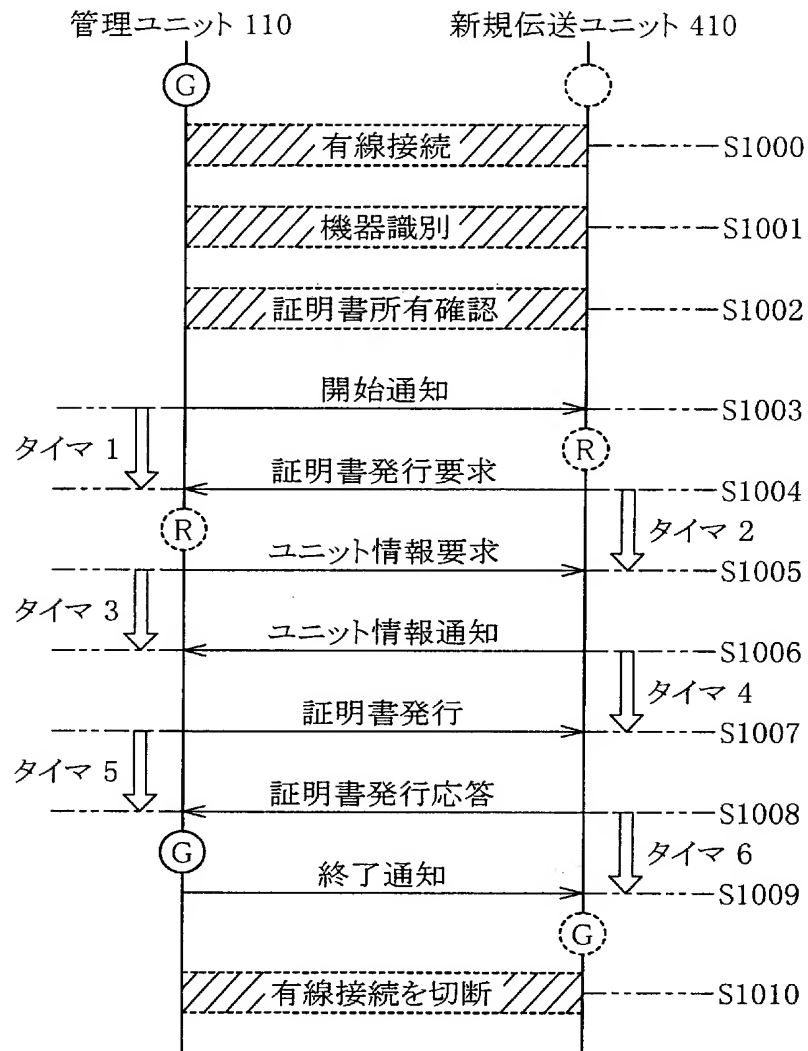
[図4]



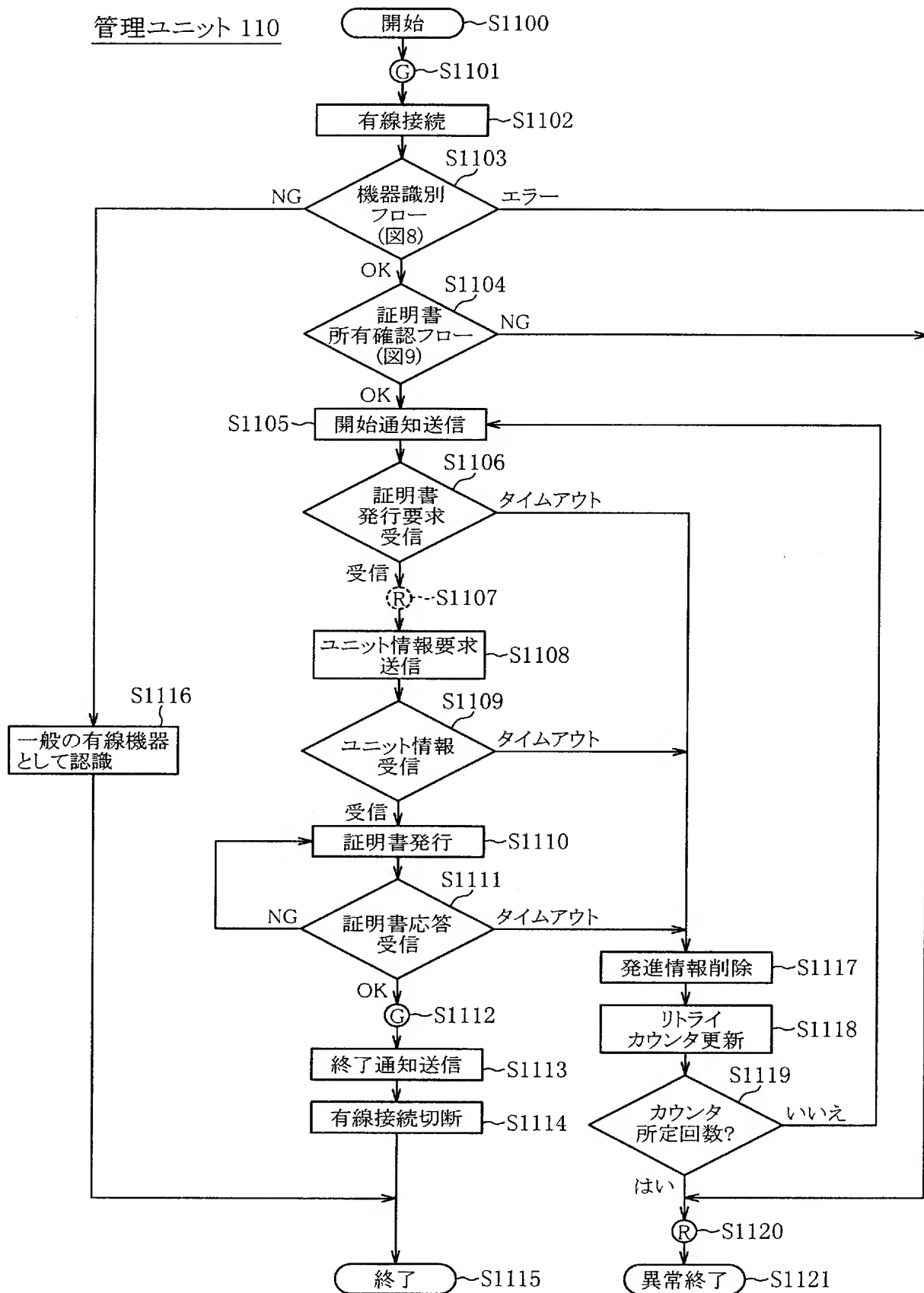
[図5]



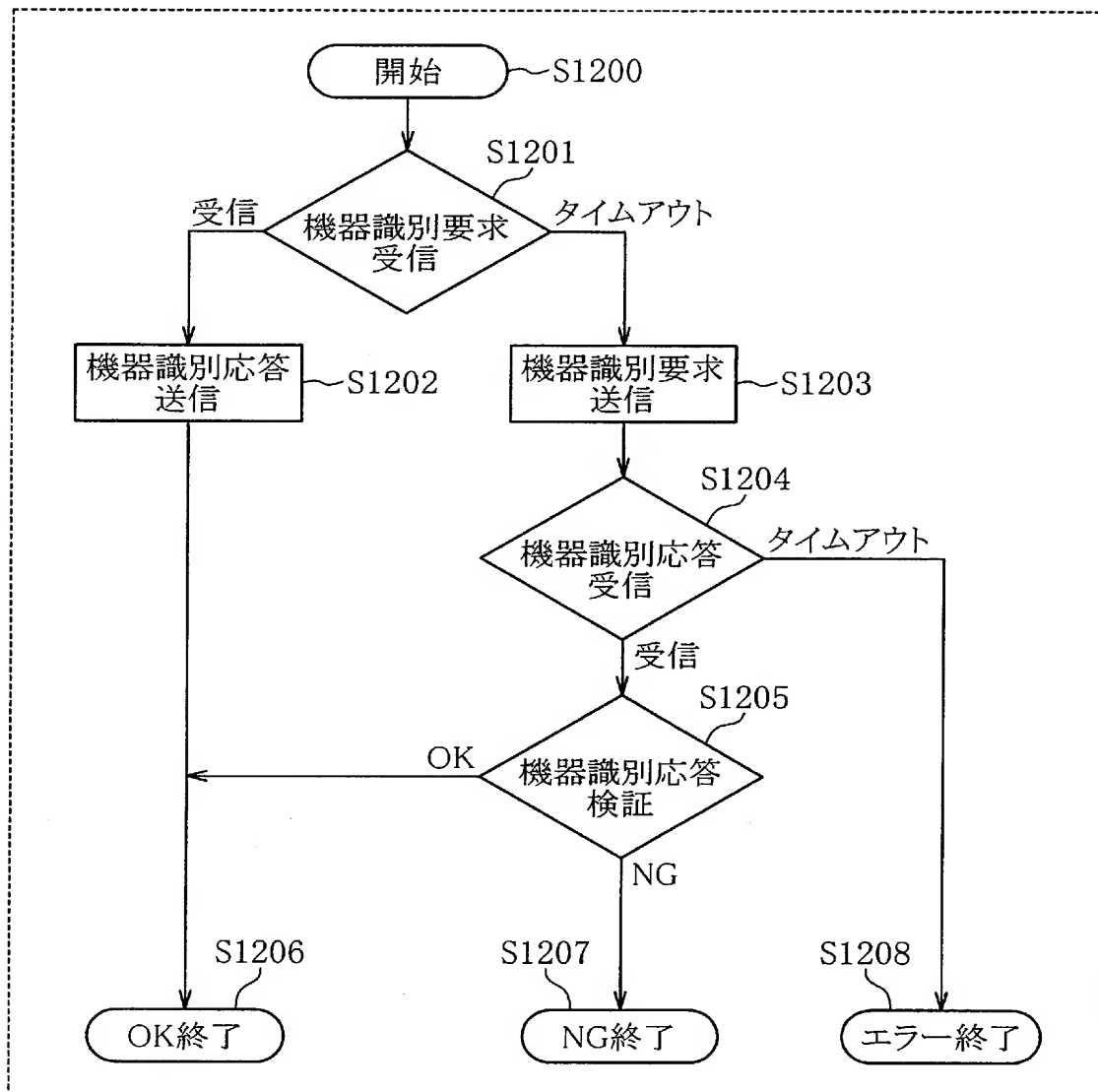
[図6]



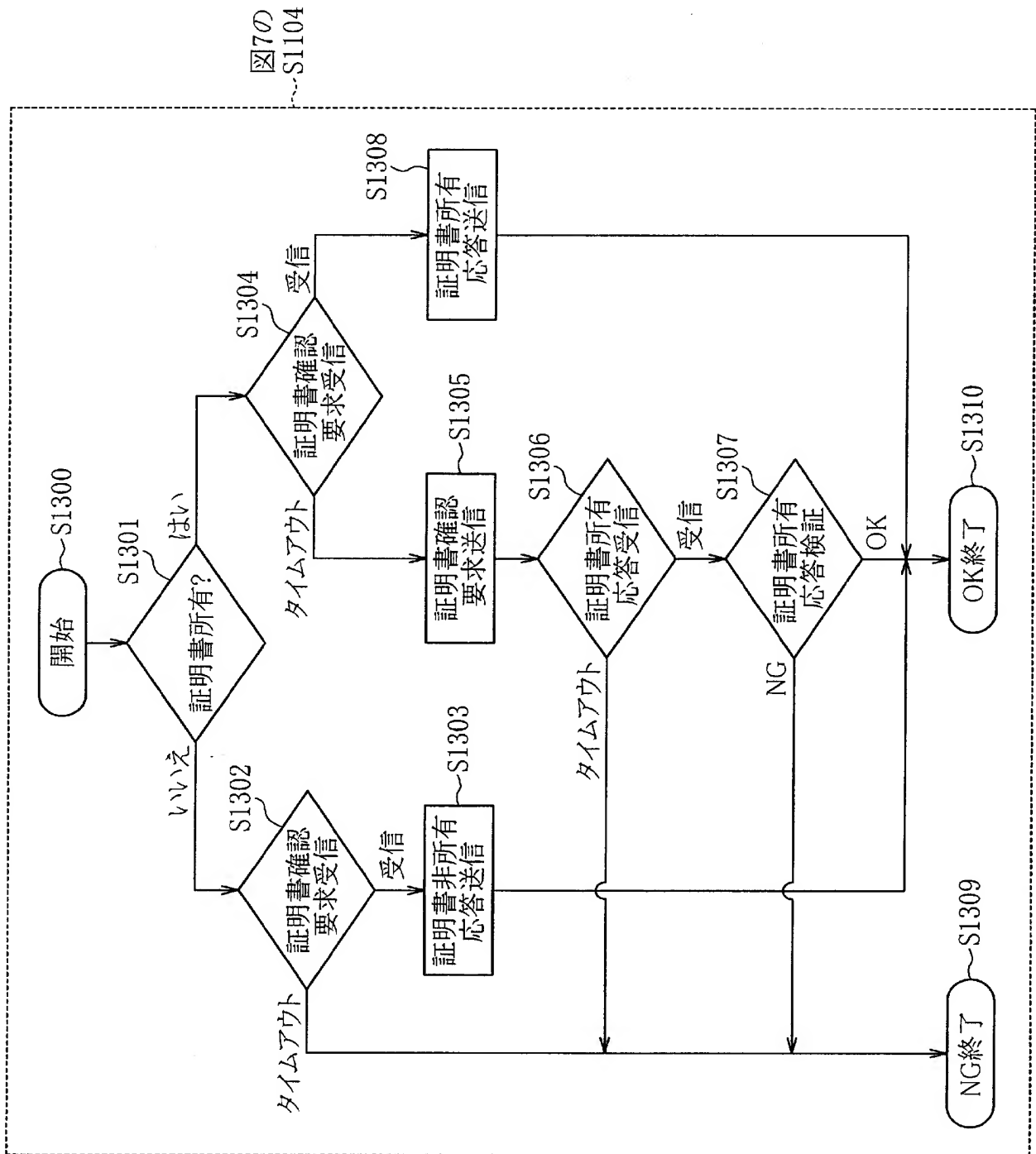
[図7]



[図8]

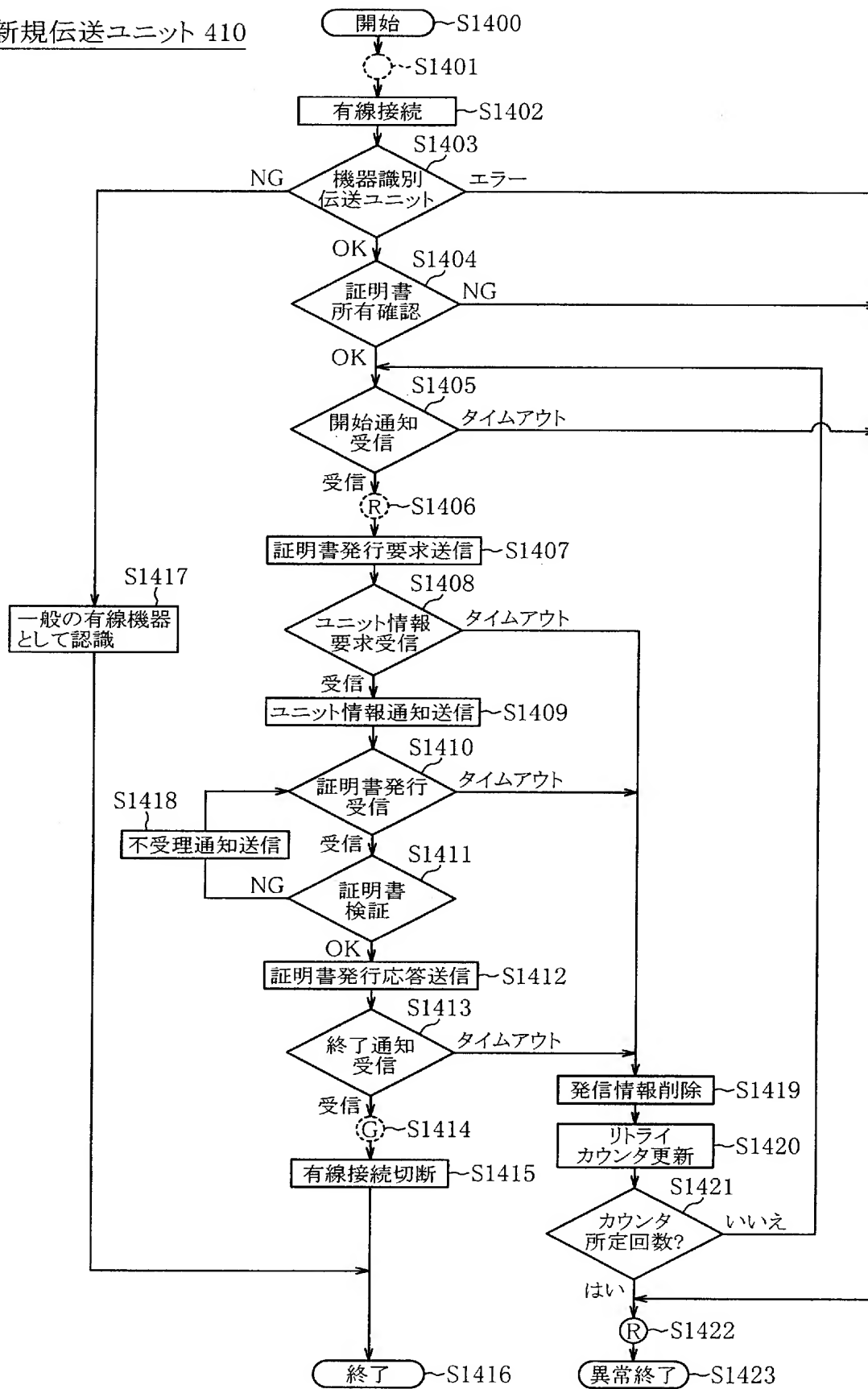
図7の
S1103

[図9]

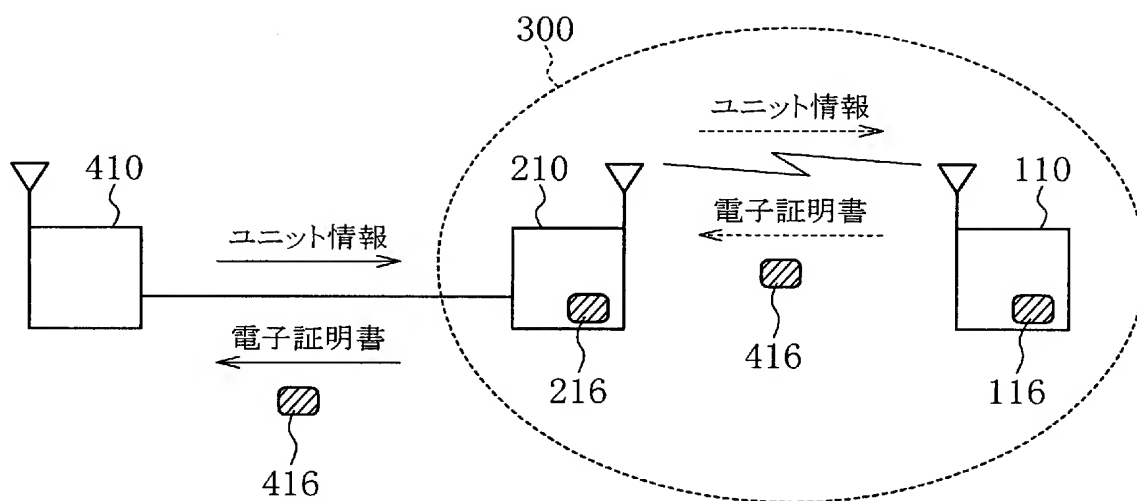


[図10]

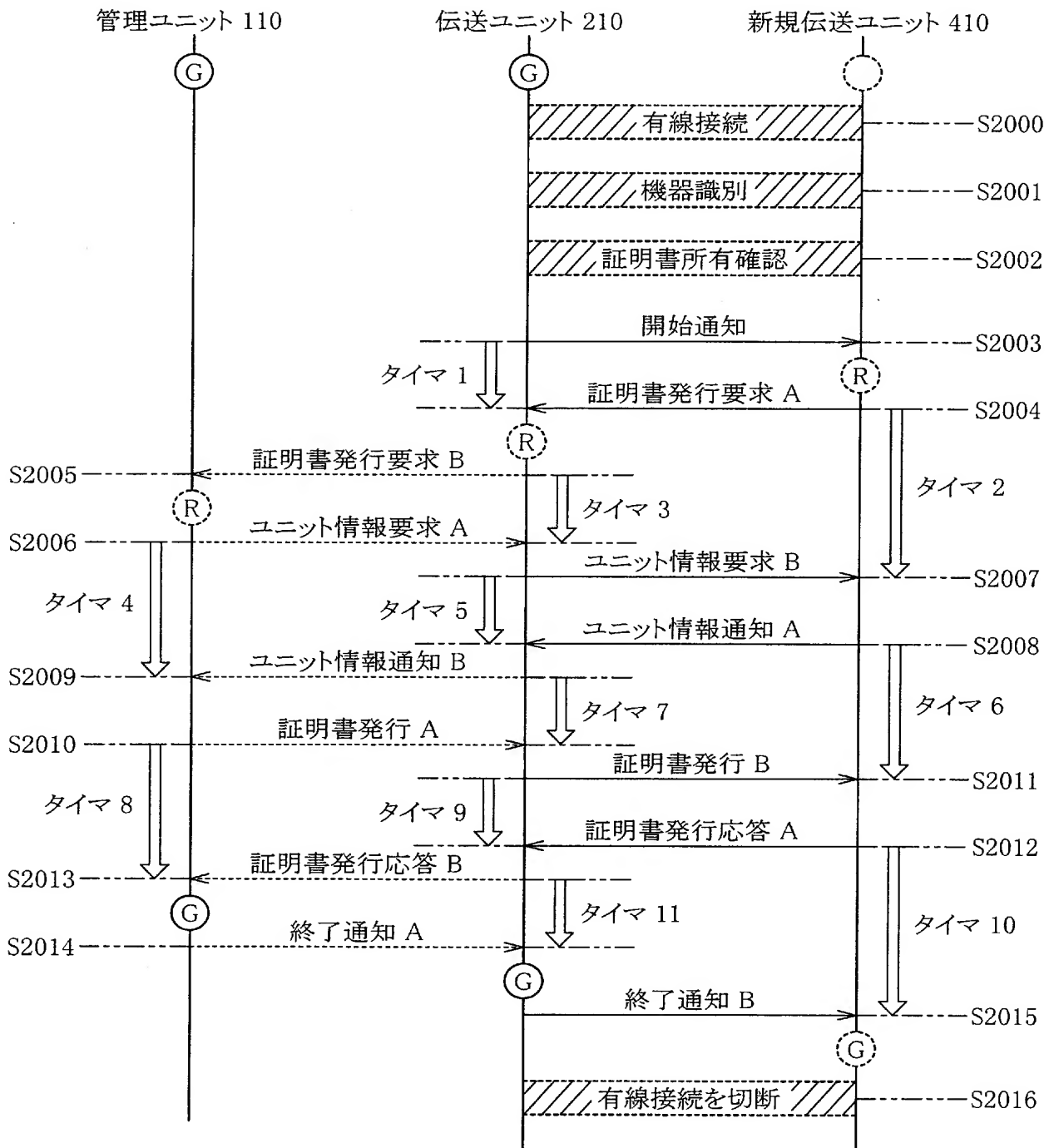
新規伝送ユニット 410



[図11]

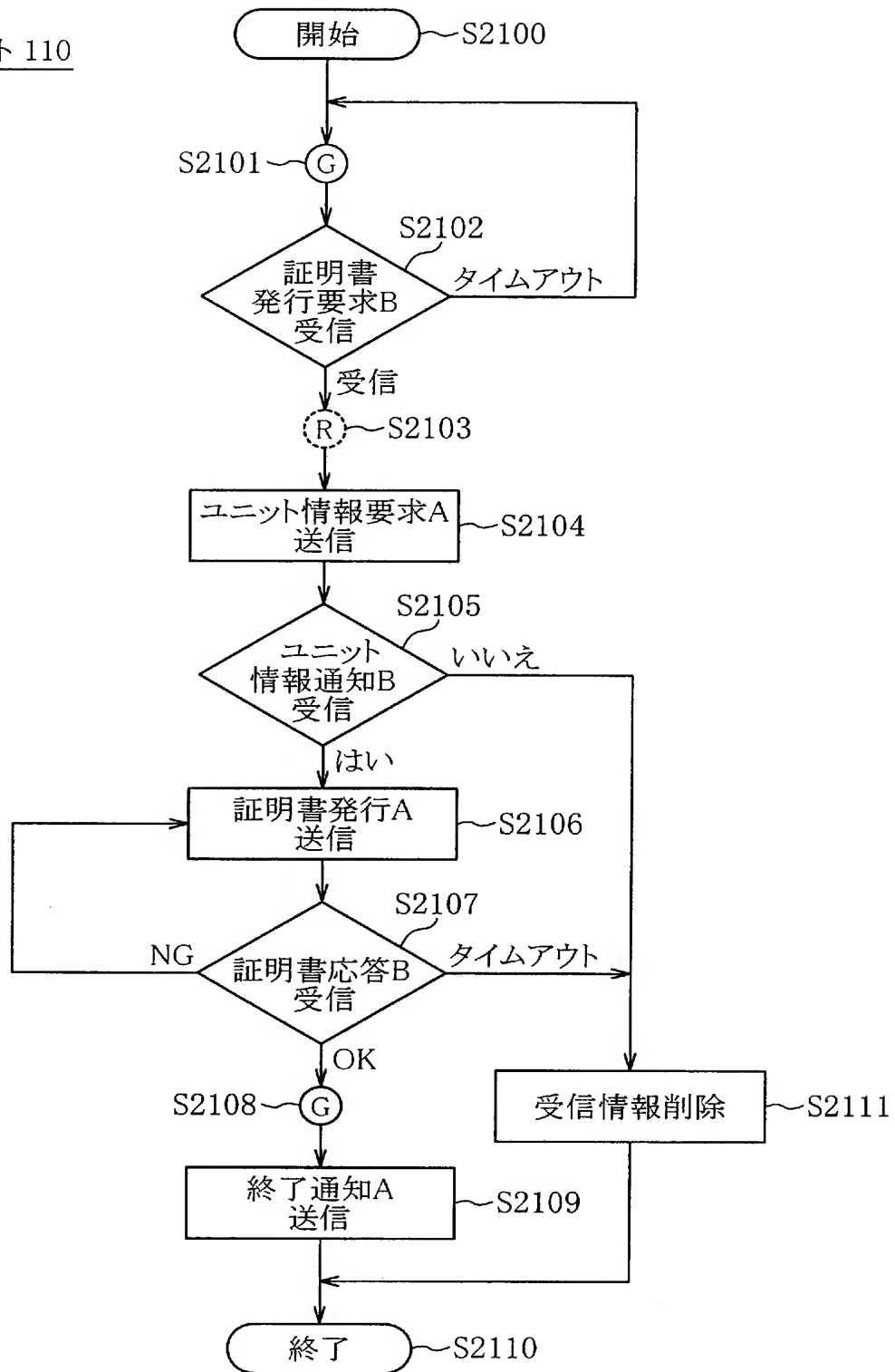


[図12]

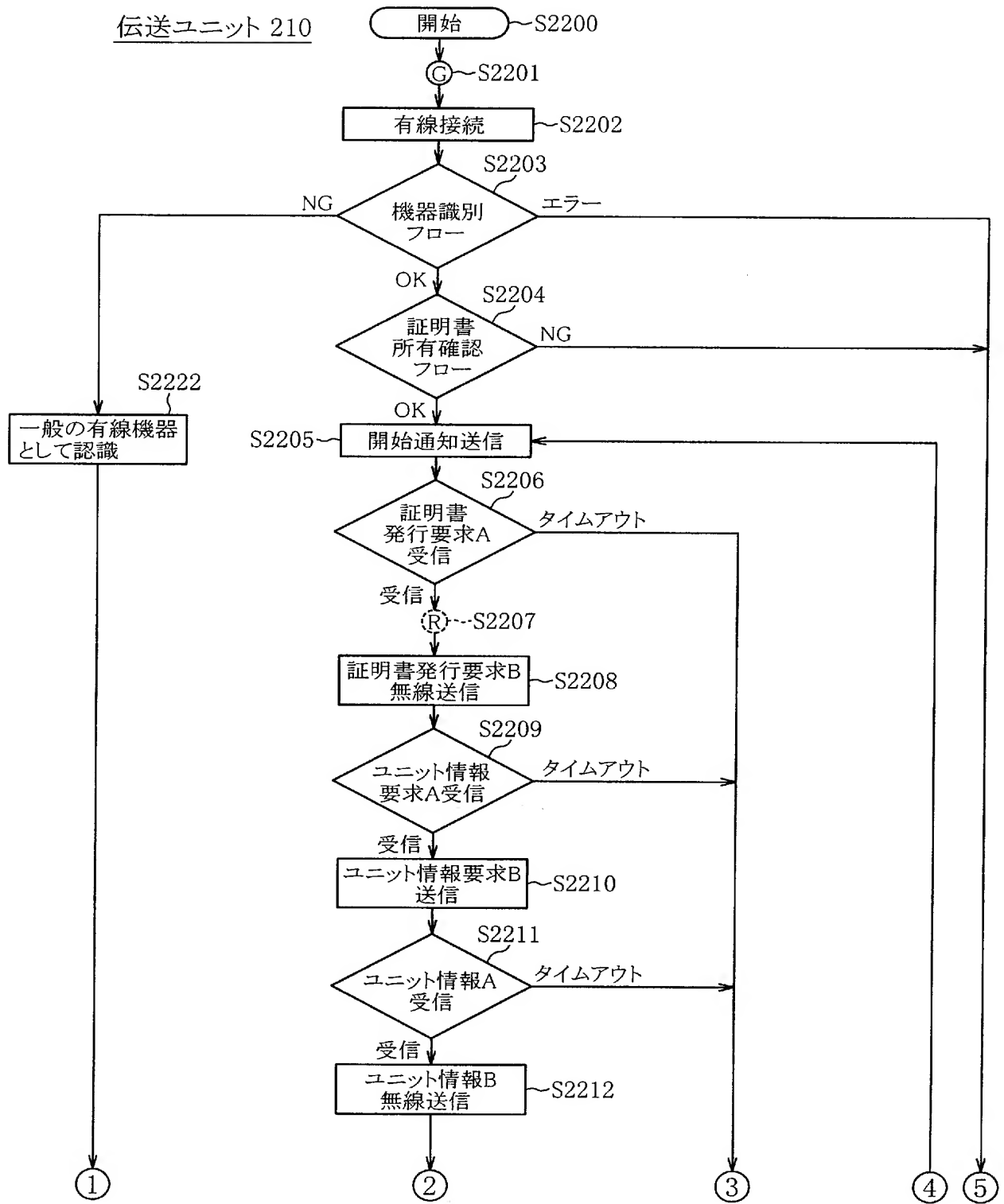


[図13]

管理ユニット 110

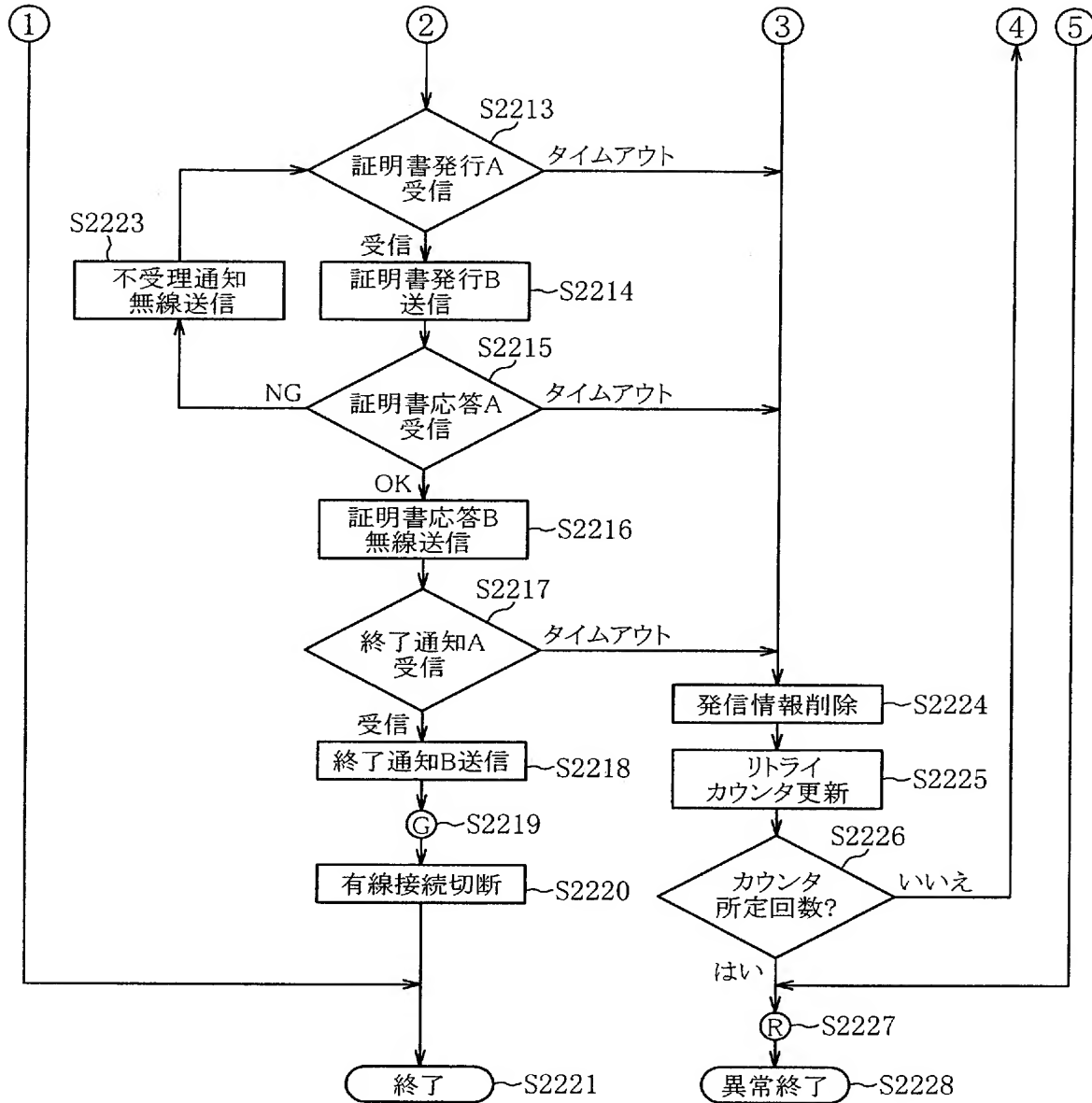


[図14]



[図15]

伝送ユニット 210



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/016388

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/08, H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/08, H04L12/28, H04B7/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS), WPI, certificate, ad hoc network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-500923 A (International Business Machines Corp.), 07 January, 2003 (07.01.03), Par. Nos. [0030], [0037] to [0038], [0042], [0043] & WO 00/072506 A1 & AU 200050845 A & CN 1351789 A & CZ 200104168 A3 & EP 1179244 A1 & HU 200201561 A2 & KR 2001114272 A & TW 478269 A & TW 480864 A & TW 498969 A & US 6772331 B1	1, 4, 7, 10, 11, 14
Y	JP 07-336370 A (Toshiba Corp.), 22 December, 1995 (22.12.95), Par. Nos. [0029] to [0054] & EP 680174 A2 & US 5771352 A	1, 4, 7, 10, 11, 14

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 March, 2005 (25.03.05)

Date of mailing of the international search report
12 April, 2005 (12.04.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/016388

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol.2, No.1, 2003, March, pages 52 to 64, especially 1 INTRODUCTION, 3.1 Creation of Public Keys and Public-Key Certificates	1, 7, 10
Y	JP 2003-188873 A (Kanazawa Institute of Technology), 04 July, 2003 (04.07.03), Par. Nos. [0061] to [0064], [0066] to [0070], [0075] (Family: none)	10, 14
A	JP 2003-309558 A (Xerox Corp.), 31 October, 2003 (31.10.03), Par. Nos. [0020] to [0022] & EP 1335563 A2 & US 2003/149874 A1	1-14
A	JP 2002-359623 A (Seiko Epson Corp.), 13 December, 2002 (13.12.02), Par. Nos. [0120] to [0172] & CN 1378405 A & KR 2002076195 A & US 2002/147819 A1	1-14

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L12/28

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L12/28, H04B7/26

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国登録実用新案公報	1994-2005年
日本国実用新案登録公報	1996-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), WP1
certificate, ad hoc network

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2003-500923 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2003.01.07 第30, 37-38, 42, 43段落 & WO 00/072506 A1 & AU 200050845 A & CN 1351789 A & CZ 200104168 A3 & EP 1179244 A1 & HU 200201561 A2 & KR 2001114272 A & TW 478269 A & TW 480864 A & TW 498969 A & US 6772331 B1	1, 4, 7, 10, 11, 14
Y	JP 07-336370 A (株式会社東芝) 1995.12.22 第29-54段落 & EP 680174 A2 & US 5771352 A	1, 4, 7, 10, 11, 14

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

25.03.2005

国際調査報告の発送日

12.4.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 2, NO. 1, 2003年3月, p. 52-64, especially 1 INTRODUCTION, 3.1 Creation of Public Keys and Public-Key Certificates	1, 7, 10
Y	JP 2003-188873 A (学校法人金沢工業大学) 2003. 07. 04 第61-64, 66-70, 75段落 (ファミリなし)	10, 14
A	JP 2003-309558 A (ゼロックス・コーポレーション) 2003. 10. 31 第20-22段落 & EP 1335563 A2 & US 2003/149874 A1	1-14
A	JP 2002-359623 A (セイコーエプソン株式会社) 2002. 12. 13 第120-172段落 & CN 1378405 A & KR 2002076195 A & US 2002/147819 A1	1-14